ThinkVantage

ThinkVantage テクノロジー デプロイメント・ガイド

更新: 2005年10月14日

以下を含みます。

- Rescue and Recovery バージョン 3.0
- Client Security Solution バージョン 6.0
- 指紋認証ユーティリティー・バージョン 4.6

ThinkVantage

ThinkVantage テクノロジー デプロイメント・ガイド

更新: 2005年10月14日

第1刷 2005.10

目次

第 7 章 Antidote Delivery Manager のインフラストラクチャー 121

第 8 章 ベスト・プラクティス 127

第 9 章 指紋認証ユーティリティー . . 145

付録 A. インストール・コマンド・ライン・パラメーター 153

付録 B. TVT.TXT の設定および値 . . . 157

付録 C. コマンド・ライン・ツール. . . 171

付録 D. 管理者ツール 187

まえがき

本書は、IT 管理者、または Rescue and Recovery™ プログラムを組織内の PC にデプロイする担当者を対象としています。 Rescue and Recovery のゴールは、ヘルプ・デスクのコールおよびデスクサイドへの訪問を回避してコストを削減し、ユーザーの生産性を改善することにあります。これは、Microsoft® Windows® オペレーティング・システムが立ち上がらない、あるいは正しく稼動しない場合に、ユーザーおよび管理者がバックアップからの復元、ファイルへのアクセス、問題の診断、およびイーサネット接続を行うことができるツールです。また、破壊されたかまたはネットワーク上にないシステムへのクリティカルな更新のデプロイメントを可能にし、復元の実行時に自動的にシステムへパッチを適用します。本書は、Rescue and Recovery を 1 台以上の PC にインストールするために必要な情報を提供します。各ターゲット PC で同ソフトウェアのライセンスが有効であることが条件となります。また、IT または企業方針をサポートするためにカスタマイズすることができるツールの多くの特徴についての情報を提供しています。 Rescue and Recovery ワークスペースに組み込まれているさまざまなコンポーネントの使用に関する質問および情報は、そのコンポーネントのオンライン・ヘルプ・システムを参照してください。

Rescue and Recovery は、機能およびアプリケーション・ヘルプを提供します。 Rescue and Recovery ワークスペースに組み込まれているさまざまなコンポーネントの使用に関する質問および情報は、そのコンポーネントのオンライン・ヘルプ・システムを参照してください。

このデプロイメント・ガイドは、IT プロフェッショナルにより固有の目標を念頭に作成されています。ご提案またはコメントは、Lenovo 認定担当者にご連絡ください。本書は定期的に更新されます。より新しいバージョンについては、次の Web サイトを参照してください。

http://www.lenovo.com/ThinkVantage (英語のサイトです。)
http://www.ibm.com/jp/pc/think/thinkvantagetech.shtml (日本語のサイトです。)

第 1 章 概要

本書の対象読者は、社内セキュリティー・テクノロジーの実装と配置を担当する、IT セキュリティー、管理およびその他の担当者です。 ThinkVantage™ Rescue and Recovery は、 ThinkVantage テクノロジー製品のうちの 1 製品です。このアプリケーションは、Microsoft® Windows オペレーティング・システムが起動しない場合であっても使用できるツール群から構成されています。

これらのテクノロジーは、企業環境で IT プロフェッショナルを直接的および間接的に支援します。すべての ThinkVantage テクノロジーは、 PC の使い勝手と自己完結性を向上させ、ロールアウトを促進し単純化する強力なツールを提供するので、 IT プロフェッショナルには大きなメリットをもたらします。 ThinkVantage テクノロジーを継続的に使用すると、IT プロフェッショナルは、個別の PC の問題を解決する時間を短縮できるので、中核となる作業に多くの時間を費やすことができるようになります。

主要なコンポーネント

本書の主要なコンポーネントは、以下のとおりです。

- ThinkVantage Rescue and Recovery
- ThinkVantage Client Security Solution
- ThinkVantage 指紋認証ユーティリティー

それぞれについての説明は、以下のとおりです。

Rescue and Recovery

Rescue and Recovery には、以下の 2 つの主要なコンポーネントがあります。

- Windows オペレーティング・システムとは独立させて起動することができる Rescue and Recovery ワークスペース。
- Rescue and Recovery (Windows 環境): バックアップ、ファイルのレスキュー、およびオペレーティング・システムおよびファイルのリカバリーをすることができます。

注: Rescue and Recovery には、Windows オペレーティング・システムで実行される機能があり、Windows の実行中に Rescue and Recovery ワークスペースで使用されるシステム情報なども収集されます。Windows オペレーティング・システムが誤動作しても、 Rescue and Recovery ワークスペースの正常な動作が妨げられることはありません。ただし、Windows オペレーティング・システムで実行される機能について、本デプロイメント・ガイドでは説明しません。

Rescue and Recovery ワークスペース

Rescue and Recovery ワークスペースは、エンド・ユーザーの PC で Windows を起動できない場合の緊急用の作業環境を提供します。この環境は Rescue and Recovery

ワークスペース (Preinstallation Environment) ベースのプログラムなので、Windows のような外観および機能を提供し、エンド・ユーザーは IT スタッフの時間を取らずに問題を自己解決できます。

Rescue and Recovery ワークスペースには、以下の 4 つの主要カテゴリーの機能があります。

- **レスキューおよび復元**
  - **復元の概要:** さまざまなリカバリー・オプションに関するヘルプ・トピックへのリンクを提供します。
  - **ファイルのレスキュー:** Windows 上に保存されているファイルを外部メディアまたはネットワーク上の共有フォルダーにコピーし、使用不可のワークステーションとも一緒に作業を続けられます。
  - **システムの復元:** Rescue and Recovery でバックアップしたファイルを復元します。また、
- **構成**
  - **構成の概要:** 設定に関する Rescue and Recovery ワークスペースのヘルプ・トピックを提供します。
  - **パスワード/パスフレーズのリカバリー:** ユーザーまたは管理者が、 Rescue and Recovery 環境でパスワードまたはパスフレーズをリカバリーできるようにします。
  - **BIOS へのアクセス:** BIOS Setup Utility プログラムを開きます。
- **通信**
  - **通信の概要:** 関連する Rescue and Recovery ワークスペースのヘルプ・トピックを提供します。
  - **ブラウザーを開く:** Opera Web ブラウザーを起動します (Web またはイントラネットにアクセスするには、有線イーサネットによる接続が必要です)。
  - **ファイルのダウンロード**
  - **ネットワーク・ドライブの割り当て:** ソフトウェアのダウンロードやファイルのレスキューを行うためにネットワーク・ドライブを割り当てます。
- **トラブルシューティング**
  - **診断の概要:** Rescue and Recovery 診断ヘルプ・トピックを提供します。
  - **ハードウェアの診断:** PC-Doctor を起動し、ハードウェア・テストを実行後、結果を報告します。
  - **診断ディスクの作成**
  - **他のデバイスから起動**
  - **システム情報:** PC およびそのハードウェア・コンポーネントに関する詳細情報を表示します。
  - **イベント・ログ:** 問題判別および解決を補助するために、 PC へのアクセス状況や PC ハードウェアのリストの詳細を提供します。このログ・ビューアーにより、イベント・ログの項目が読みやすく表示されます。
  - **保証状況**

Rescue and Recovery は、プリインストール・ソフトウェアが搭載されている Lenovo および IBM PC で使用できます。

157 ページの『付録 B. TVT.TXT の設定および値』に、 Rescue and Recovery 環境をデプロイメント用に設定する方法が記載されています。 Rescue and Recovery の

インストール時には Windows 上のコンポーネントのインストールも行いますが、本書ではそれらを、カスタマイズ、設定、およびデプロイメントの説明を行う上で個別のコンポーネントとして扱います。

Rescue and Recovery (Windows 環境)

Rescue and Recovery™ 環境では、 Windows が起動しなくなってもボタンを押すだけで、失われたデータ、アプリケーション、およびオペレーティング・システムのレスキューを行うことができます。この機能により、時間のかかるヘルプ・デスクへの呼び出し回数が減り、結果としてサポート・コストを節約できます。

また、バックアップをスケジュールすることができるので、リスクを軽減し、ダウン時間を短縮することが可能です。Rescue and Recovery は、サーバーまたは外部ストレージへの自動外部バックアップを事前設定することにより、さらなるサポートを提供することができます。

Antidote Delivery Manager

Antidote Delivery Manager は、ThinkVantage Rescue and Recovery に組み込まれたアンチウィルス、アンチワーム・インフラストラクチャーです。その目的は、素早く実行でき、効率的で、管理者が問題の報告から数分間のうちに遮断および回復作業を開始できることです。これは、1 人の管理者によって起動でき、ネットワークに接続されていないシステムでも機能します。 Antidote Delivery Manager は既存のアンチウィルス・ツールに置き換わるものではなく、それを補完するもので、ウィルス・スキャン・ツールの保守や、パッチの取得は引き続き必要です。 Antidote Delivery Manager は、破壊的活動を停止し、パッチを当てるためのインフラストラクチャーを提供します。

暗号化バックアップ

バックアップは、デフォルトで 256 AES 鍵により暗号化されます。 Client Security Solution バージョン 6.0 をインストールする場合は、Client Security Software Gina を使用して暗号化することができます。

Client Security Solution 6.0

Client Security Solution ソフトウェアの第一の目的は、お客様が資産としての PC を保護し、PC 上の機密データを保護し、さらに PC がアクセスするネットワーク接続を保護することを補助することです。 TCG (Trusted Computing Group) という業界団体が仕様を定めている TPM (Trusted Platform Module) を含む IBM® および Lenovo システムの場合、 Client Security Solution (CSS) ソフトウェアは、システムのトラステッド・ルートとしてハードウェアを活用します。システムにエンベデッド・セキュリティー・チップが含まれていない場合、 Client Security Solution は、システムのトラステッド・ルートとしてソフトウェア・ベースの暗号化鍵を活用します。 Client Security Solution 6.0 には、以下の機能が含まれています。

- **セキュアなユーザー認証**

  ハードウェアで保護された Client Security パスフレーズが必要です。ユーザーは、このパスフレーズを使用して Client Security Solution で保護された機能にアクセスします。

- **指紋によるユーザー認証**

  内蔵型および USB 接続の指紋テクノロジーを活用し、パスワードで保護されたアプリケーションに対してユーザーを認証します。

- **Client Security パスフレーズ/指紋による Windows ログオン**

  ユーザーは、ハードウェアで保護された Client Security パスフレーズまたは指紋を使用して、 Windows にログオンする必要があります。

- **データの保護**

  ハードディスク上のセキュアな場所に保管することにより、機密ファイルを暗号化します。この場合は、有効なユーザー認証と適切に構成されたセキュリティー・チップが必要になります。

- **ログオン・パスワードの管理**

  ユーザー ID やパスワードなどの重要なログオン情報を安全に管理し、保管します。

- **エンド・ユーザーのパスワード/パスフレーズのリカバリー**

  ユーザーが、Windows のパスワード/Client Security パスフレーズを忘れた場合に、事前構成された質問に答えることで、自分でリカバリーできるようにします。

- **セキュリティー設定の監査**

  ユーザーが、詳細なワークステーション・セキュリティー設定値のリストを表示し、定義された規格に準拠するように変更できるようにします。

- **ディジタル証明書の転送**

  ハードウェアは、ユーザーと PC の証明書の秘密鍵を保護します。

Client Security パスフレーズ

Client Security パスフレーズは、Client Security Solution アプリケーションに拡張セキュリティーを提供する、ユーザー認証のオプションの追加フォームです。 Client Security パスフレーズの要件は、以下のとおりです。

- 8 文字以上の長さ
- 数字が 1 文字以上入っていること
- 最近の 3 回のパスフレーズと異なること
- 反復文字は 2 文字以内
- 先頭に数字を使用しない
- 末尾に数字を使用しない
- ユーザー ID を含めない
- 現在のパスフレーズを設定してから 3 日以内は変更しない
- 現在のパスフレーズと同一の文字を連続して 3 文字以上使用しない
- Windows パスワードと異なる

同じタイプのアタックがあった場合、 Windows パスワードは受け入られますが、Client Security パスフレーズは受け入れられません。 Client Security パスフレーズ

を知っているのは個々のユーザーだけであり、 Client Security パスフレーズを忘れた場合にリカバリーする唯一の方法は、 Client Security パスワード・リカバリー機能の活用であることに注意してください。ユーザーがリカバリーの質問に対する回答を忘れてしまった場合、 Client Security パスフレーズで保護されたデータをリカバリーする方法はありません。

Client Security パスワードのリカバリー

このオプションの設定を使用すると、登録されたユーザーは、 Windows パスワードや Client Security パスフレーズを忘れた場合に、 3 つの質問に正しく答えることにより、リカバリーすることができます。この機能が使用可能である場合、エンド・ユーザーの Client Security 登録中に、各ユーザーは、事前選択された 10 の質問に対して回答を 3 つ選択することができます。ユーザーがこれまでに自分の Windows パスワードや Client Security パスフレーズを忘れたことがある場合は、これら 3 つの質問に回答して、そのパスワードやパスフレーズを自分でリセットするというオプションが用意されています。

注:

1. Client Security パスフレーズを使用する場合、これは忘れたパスフレーズをリカバリーするための唯一のオプションです。ユーザーは、それら 3 つの質問に対する回答を忘れた場合、登録ウィザードを再実行しなくてはならず、前の Client Security 保護データはすべて失われます。
2. Client Security を使用して Rescue and Recovery ワークスペースを保護する場合、「パスワード・リカバリー」オプションによって、ユーザーの Client Security パスフレーズおよび/または Windows パスワードが実際に示されます。これは、Rescue and Recovery ワークスペースが Windows パスワードの変更を自動的に実行する機能を持たないためです。このことは、ネットワーク以外でアタックされたローカル・キャッシュ・ドメインのユーザーが、 Windows ログオンでこの機能を実行する場合にも当てはまります。

ThinkVantage 指紋認証ユーティリティー

Lenovo が提案する生物的指紋テクノロジーの目的は、パスワードの管理に関連したコストの削減やシステムに対するセキュリティーの強化においてお客様を補助し、お客様が規制に対応できるようにすることです。弊社の指紋読み取り装置とともに、 ThinkVantage 指紋認証ユーティリティーを使用すると、 PC およびネットワークに対する指紋認証が可能になります。このソリューションは、拡張機能を提供する Client Security Solution バージョン 6.0 と統合することもできます。以下のサイトには Lenovo 指紋テクノロジーについての詳細があり、ソフトウェアをダウンロードすることができます。

http://www.thinkpad.com/fingerprint (英語のサイトです。)

ThinkVantage 指紋認証ユーティリティーは、以下の機能を提供します。

- **Client Software の機能**
  - **Microsoft Windows パスワードの置換**

    パスワードをお客様の指紋に置き換えて、容易で高速、かつ安全なシステム・アクセスを提供します。

- **BIOS (パワーオン・パスワードとも呼ばれます) およびハードディスク・パスワードの置換**

  これらのパスワードをお客様の指紋と置き換えて、ログオン・セキュリティーと利便性を高めます。

- **Windows へのシングル・スワイプ・アクセス:**

  ユーザーは、始動時に指紋を一度指紋を読取装置に通すだけで、 BIOS と Windows にアクセスすることができるので、貴重な時間を節約することができます。

- CSS Password Manager と併用して、 TPM を活用するための **Client Security Solution との統合**。ユーザーは、自分の指紋を読取装置に通して Web サイトにアクセスし、アプリケーションを選択します。

- **管理者機能**
  - **セキュリティー・モードの切り替え:**

    管理者は、セキュア・モードと便利モードを切り替えて、制限ユーザーのアクセス権限を変更することができます。

  - **管理コンソール:**

    スクリプト駆動コマンド・ライン・インターフェースにより指紋認証ユーティリティーのリモート・ソフトウェアのカスタマイズを可能にして、管理者を補助します。

- **セキュリティー機能**
  - **ソフトウェア・セキュリティー:**

    システムに保管する際や、読み取り装置からソフトウェアに転送する際に、強い暗号化により、ユーザー・テンプレートを保護します。

  - **ハードウェア・セキュリティー:**

    読み取り装置には、指紋テンプレート、 BIOS パスワードおよび暗号化鍵を保管し保護するセキュリティー・コプロセッサーがあります。

Password Manager

Client Security Password Manager を使用すると、ユーザー ID、パスワード、およびその他の個人情報などの、重要だが忘れやすいアプリケーションや Web サイトのログイン情報を管理し、記憶することができます。 Client Security Password Manager は、ユーザーのアプリケーションや Web サイトへのアクセス全体がセキュアに保たれるように、エンベデッド・セキュリティー・チップを介してすべての情報を保管します。

つまり、個々のパスワードを多数記憶したり指定しなくても (この場合、規則や有効期限の日付はさまざまです)、 1 つのパスワード/パスフレーズを覚えておき、指紋を提供するか、識別要素の組み合わせを指定すればよいということです。

Client Security Password Manager を使用すると、以下の機能を実行できます。

- **エンベデッド・セキュリティー・チップによるすべての保管情報の暗号化**

Client Security Password Manager は、エンベデッド・セキュリティー・チップを介してすべての情報を自動的に暗号化します。これにより、すべての重要なパスワード情報が、Client Security Solution 暗号化鍵によって保護されます。

- **ユーザー ID とパスワードの高速転送および使いやすい単純な入力転送インターフェース**

  Client Security Password Manager の入力転送インターフェースを使用すると、ブラウザーまたはアプリケーションのログオン・インターフェースに直接情報を入力することができます。これにより、入力エラーを最小化し、エンベデッド・セキュリティー・チップを介してすべての情報を安全に保存することができます。

- **自動キーのユーザー ID とパスワード**

  Client Security Password Manager は、ログオン情報がすでに Client Security Password Manager に入力されているアプリケーションや Web サイトにアクセスする際に、ログイン情報を自動的に入力して、ログイン・プロセスを自動化します。

- **ランダム・パスワードの生成**

  Client Security Password Manager を使用すると、各アプリケーションや Web サイト用にランダム・パスワードを生成できます。これにより、各アプリケーションでより堅固なパスワード保護が可能になるため、データのセキュリティーを高めることができます。ランダム・パスワードは、ユーザー定義のパスワードよりはるかに安全です。これは、経験上、ほとんどのユーザーが覚えやすい個人情報をパスワードに使用しており、比較的容易に解読されてしまうからです。

- **Client Security Password Manager インターフェースを使用した項目の編集**

  Client Security Password Manager を使用すると、すべてのアカウント項目を編集し、すべてのオプションのパスワード機能を 1 つの使いやすいインターフェースにセットアップすることができます。これにより、パスワードと個人情報の管理を迅速かつ容易に行えるようになります。

- **Microsoft(R) Windows(R) デスクトップのアイコン・トレイから、または単純なキーボード・ショートカットを使用したログオン情報へのアクセス**

  Password Manager アイコンを使用すると、別のアプリケーションや Web サイトを Password Manager に追加する必要があるときに、いつでも容易にログオン情報へのアクセスできるようになります。 Client Security Password Manager の各機能にも、単純なキーボード・ショートカットによって容易にアクセスできます。

- **ログイン情報のエクスポートとインポート**

  Client Security Password Manager を使用すると、重要なログイン情報をエクスポートして、その情報を PC 間で安全に移動させることができます。 Client Security Password Manager からログイン情報をエクスポートすると、パスワードで保護されたエクスポート・ファイルが作成されます。このファイルは、取り外し可能メディアに保管することができます。このファイルを使用して、あらゆる場所でユーザー情報とパスワードにアクセスしたり、 Password Manager を使用して項目を別の PC にインポートします。

注: インポートが機能するのは Client Security Solution バージョン 6.0 のみです。 Client Security Software バージョン 5.4X 以前のバージョンは、 Client Security Solution 6.0 Password Manager にインポートされません。

SafeGuard PrivateDisk

SafeGuard PrivateDisk を使用してデータを保護します。ほとんどの場合、機密データは PC 上に保管されます。 SafeGuard PrivateDisk は、機密データを保護します。その機能は、PC、すべてのディスク・ドライブおよびモバイル・メディア上にある重要な機密情報の「電子金庫」のようなものです。未認証の人物が保護情報にアクセスしたり、読み取ったりすることはできません。

SafeGuard PrivateDisk はどのように機能するのでしょうか? SafeGuard PrivateDisk は、仮想ディスクの原理に基づいています。

- 仮想ディスクは、使用可能なあらゆるドライブ上に作成することができます。
  - モバイル・メモリー・メディア (ディスク、USB スティック、CD-ROM、DVD、または Zip ドライブなど)
  - ハードディスク、ネットワーク・ドライブ
- ドライバーは、ハードディスクのように機能します。
  - オペレーティング・システムは、書き込みおよび読み取りコマンドをドライバーに透過的に送信します。
  - ドライバーは、暗号化されたストレージを管理します。
  - データとディレクトリー情報は、すべて暗号化されます。
- SafeGuard PrivateDisk は、Client Security Solution および TPM とともに機能し、PrivateDisk で生成されたディジタル証明書を保護します。
- SafeGuard PrivateDisk は、対称暗号アルゴリズムと各仮想ディスク用の新しいランダム AES 鍵を併用します。
  - AES、128 ビット、CBC モード
  - 各仮想ディスク用の新しいランダム鍵
- 認証は、以下を介して行われます。
  - パスワード
  - 秘密鍵 (X.509 証明書)、オプションのスマート・カード
  - 自動生成された EFS 証明書を使用できます
- パスワード・セキュリティーは、以下のとおりです。
  - PKCS#5
  - 不正なパスワードの提示による時刻の遅延
  - 「インターセプト保護」を表示するパスワード・ダイアログ

Security Advisor

Security Advisor ツールを使用すると、現在 PC に設定されているセキュリティー設定値の要約を表示できます。これらの設定値を検討して、現在のセキュリティー状況を表示したり、システム・セキュリティーを強化することができます。含まれているセキュリティー・トピックの中には、ハードウェア・パスワード、 Windows

ユーザー・パスワード、 Windows パスワード・ポリシー、保護スクリーン・セーバー、およびファイル共用があります。表示されるカテゴリーのデフォルト値は、TVT.txt ファイルによって変更できます。

証明書転送ウィザード

Client Security の証明書転送ウィザードは、ソフトウェア・ベースの Microsoft 暗号サービス・プロバイダーからハードウェア・ベースの Client Security Solution CSP に、証明書に関連した秘密鍵を転送するすべてのプロセスをガイドします。転送が行われた後は、秘密鍵がエンベデッド・セキュリティー・チップによって保護されるため、証明書を使用する操作はよりセキュアになります。

ハードウェア・パスワードのリセット

このツールは、Windows とは独立して稼動するセキュアな環境を作成し、忘れてしまったパワーオン・パスワードやハードディスク・パスワードをリセットする際に役立ちます。 ID は、自分で作成した一連の質問に回答することによって設定されます。パスワードを忘れてしまわないうちに、このセキュアな環境をできるだけ早く作成することをお勧めします。登録後、ハードディスク上にこのセキュアな環境を作成するまでは、忘れてしまったハードウェア・パスワードをリセットすることはできません。このツールは、ThinkCentre® と ThinkPad PC を選択した場合のみ、使用可能です。

TPM のないシステムのサポート

Client Security Solution 6.0 は現在、対応するエンベデッド・セキュリティー・チップのない IBM および Lenovo システムをサポートしています。これにより、均質的なセキュリティー環境を作成するために、全社的な標準インストールを行うことが可能になります。組み込みセキュリティー・ハードウェアを持つシステムは、アタックに対して、より堅固ですが、追加のセキュリティーと機能性もソフトウェア専用 PC にとって有益です。

System Migration Assistant

System Migration Assistant (SMA) は、システム管理者がユーザーの作業環境を、あるシステムから別のシステムに移行する場合に使用できるソフトウェア・ツールです。ユーザーの作業環境には、以下のものがあります。

- オペレーティング・システム設定 (たとえば、デスクトップおよびネットワーク接続設定)
- ファイルとフォルダー
- カスタマイズされたアプリケーション設定 (たとえば、Web ブラウザーのブックマーク、 Microsoft Word の編集設定)
- ユーザー・アカウント

システム管理者は SMA を使用して、企業の標準作業環境をセットアップしたり、個々のユーザーの PC をアップグレードしたりできます。個々のユーザーは SMA を使用して、PC をバックアップしたり、設定とファイルを 1 つの PC システムから別の PC システムに移行したりできます。たとえば、デスクトップ PC からモバイル PC (ラップトップ) に移行することができます。

OEM の違い

Client Security Solution 6.0 は、現時点では OEM システムでは使用できません。Rescue and Recovery は、 OEM PC では Client Security Solution アプリケーションを活用できません。

第 2 章 インストールの考慮事項

ThinkVantage Rescue and Recovery をインストールする前に、アプリケーション全体のアーキテクチャーを理解する必要があります。

Rescue and Recovery

Rescue and Recovery には 2 つの主要なインターフェースがあります。 1 つめのインターフェースは Windows XP または Windows 2000 環境で作動します。 2 つめのインターフェース (Rescue and Recovery ワークスペース) は、Rescue and Recovery ワークスペース環境で、Windows XP または Windows 2000 オペレーティング・システムのいずれとも独立して作動します。

注:

1. Rescue and Recovery が最初にインストールされて、次に Computrace がインストールされた場合、Rescue and Recovery は Computrace の非 BIOS バージョンとのみ連動します。 127 ページの『第 8 章 ベスト・プラクティス』を参照してください。
2. 仮想パーティションとしてインストール済みの Rescue and Recovery ワークスペース領域でインストールされた Rescue and Recovery を使用するシステム上で SMS のインストールを試みた場合、SMS はインストールしません。 Rescue and Recovery ワークスペースと SMS は両方とも自身のファイル・システムに C:¥minint フォルダーを使用します。同時に両方をインストールする方法は、タイプ 12 区画として Rescue and Recovery 3.0 をインストールすることです。タイプ 12 へのインストールの説明は、 142 ページの『Rescue and Recovery のタイプ 12 のサービス区画へのインストール』を参照してください。
3. 考えられるセキュリティー・リスクは、Microsoft 回復コンソール が Rescue and Recovery を持つシステム上でインストールされるときに起こります。 Microsoft 回復コンソールは、パス C:¥*¥system32¥config¥ ですべてのフォルダーを検索し、このパスが検出された場合はそれがオペレーティング・システムであると仮定します。 Windows パスワードを要求するレジストリー項目がない場合、回復コンソールはユーザーにオペレーティング・システムの選択を許可し、パスワードを入力することを必要とせずにハードディスク全体へのアクセスを取得します。

上書きインストールの考慮事項

Rescue and Recovery バージョン 3.0 は、Rescue and Recovery 2.0 の上書きインストールをサポートしています。

Rescue and Recovery 3.0 のインストール後、新規でバックアップを取り直すようお勧めします。これは、スクリプトまたはユーザー・インターフェースを使用して行うことができます。

以下は、新規にバックアップを取り直す際に行う標準的な手順です。

1. 以前のバックアップを保存しておきたい場合は、事前に CD/DVD ドライブまたは USB HDD ドライブにコピーします。
2. 現行のバックアップを削除します。
3. 基本バックアップを実行します。

次のスクリプトは、USB HDD にバックアップをコピーし、現行バックアップを削除、最後に基本バックアップを実行します。

```
@echo off

::Change directories to ¥Program Files¥IBM¥IBM Rescue and Recovery
cd %rr%

::copy backups to the USB drive
rrcmd copy location=U

::Delete All backups from local HDD silently
rrcmd delete location=L level=0 silent

::Perform a New Base Backup to local HDD silently
rrcmd backup location=L name="Rescue and Recovery 2.0 Base" silent
```

Client Security Solution

Client Security Solution 6.0 をデプロイするときは、以下の側面を考慮しなければなりません。

Client Security Solution はそのコード内に必要なドライバーとソフトウェア・サポートを含み、Client Security Solution 6.0 を受信する PC のセキュリティー・ハードウェア (TPM) を使用可能にします。チップは実際には BIOS を介して制御され、手順を完了するために正常な BIOS 認証を必要とするので、ハードウェアを使用可能にするには少なくとも 1 回再起動することが必要です。言葉を変えて言えば、BIOS 管理者/スーパーバイザー・パスワードが設定された場合は、TPM を使用可能/使用不可にする必要があります。

TPM によっていずれかの機能が実施される前に、最初に “所有権” を初期化する必要があります。各システムは、Client Security Solution オプションを制御する唯一の Client Security Solution 管理者を持ちます。この管理者は、Windows 管理者特権を持っている必要があります。管理者は XML デプロイメント・スクリプトを使用して初期化することができます。

システムの所有権が構成されたあとは、このシステムにログインする追加の各 Windows ユーザーは、ユーザーのセキュリティー・キーおよびクレデンシャルを登録し初期化するために、Client Security セットアップ・ウィザードによって自動的にプロンプトが出されます。

TPM のソフトウェア・エミュレーション

Client Security Solution は、限定されたシステム上で TPM を使用せずに実行するオプションを持っています。この機能は、ハードウェア保護キーを使用する代わりにソフトウェア・ベースのキーを使用する以外は、まったく同じです。ソフトウェアは、TPM に効力を与える代わりに、常にソフトウェア・ベースのキーを使用するよ

うに強制するスイッチでインストールすることが可能です。これはインストール時の決定で、ソフトウェアのアンインストールおよび再インストールをすることなしに戻すことはできません。

TPM のソフトウェア・エミュレーションを強制する構文は以下の通りです。

```
InstallFile.exe "/v EMULATIONMODE=1"
```

アップグレードのシナリオ

Client Security Solution の前のレベルからのアップグレードについての詳細は、 111 ページの『インストールするソフトウェアのシナリオ』を参照してください。

第 3 章 Rescue and Recovery のカスタマイズ

この章では、ThinkVantage Rescue and Recovery をカスタマイズするために使用する情報を提供しています。

デスクトップ上に「基本バックアップの作成」アイコンを配置するデプロイメントの作成

この手順を開始する前に、z062zaa1025us00.tvt、z062zaa1025jp00.tvt のような TVT ファイル (複数可) が、実行可能ファイルまたは MSI ファイルとして同じフォルダー内にあることを確認してください。そうでない場合はインストールは失敗します。ファイルの名前が setup_tvtrnr3_1027**c**.exe である場合、それは結合されたパッケージをダウンロードしたということになります。

デスクトップにユーザー用のバックアップ・アイコンを配置するデプロイメントを行うには、次のようにします。

1. SETUP_TVTRNR*XXXX*.EXE (ここで *XXXX* はビルド ID です) を一時フォルダーに展開します。

   ```
   start /WAIT setup_tvtrnrXXXX.exe /a /s /v"/qn TARGETDIR="C:¥TVTRR"" /w
   ```
2. 必要に応じて、TVT.TXT ファイルをカスタマイズします。たとえば、毎週のバックアップ・スケジュールを毎週火曜日午後 3:00 に設定するとします。これを実行するには、以下の項目を TVT.TXT の [Rescue and Recovery] セクションに追加します。 (設定について詳しくは、 157 ページの『付録 B. TVT.TXT の設定および値』を参照してください。)

   ```
   ScheduleHour=15
   ScheduleMinute=00
   ScheduleDayOfTheWeek=2
   ```
3. Z062ZAA1025US00.TVT と Z062ZAA1025JP00.TVT ファイルも同様に C:¥tvtrr へコピーします。 TVT ファイルは MSI ファイルと同じフォルダー内にある必要があります。
4. コマンド・プロンプトから以下を実行して、再起動をしない MSI インストールを行います。

   ```
   start /WAIT msiexec /i "C:¥TVTRR¥Rescue and Recovery - client security
   solution.msi" /qn REBOOT="R" /L*v %temp%¥rrinstall.txt
   ```

   注: 上記のコマンドはこのページに入るように修正されています。このコマンドを 1 行として入力してください。
5. Rescue and Recovery 環境をカスタマイズします。 (詳しくは、 22 ページの『ワークスペース (Predesktop area)』を参照してください。)
6. C:¥TVTRR フォルダー内の一時ファイルを除外します。 (19 ページの『Windows 環境』を参照してください)。
7. 以下が記述されたコマンド・ファイルを作成します。

   ```
   del "c:¥Documents and Settings¥All Users¥Desktop¥Create Base Backup.lnk
   "%RR%rrcmd.exe" backup location=L name=Base level=0
   ```


注: 上記のコマンドはこのページに入るように修正されています。このコマンドを 1 行として入力してください。

8. 「Document and Settings」→「All Users」→「デスクトップ」フォルダーに「基本バックアップの作成」というショートカットを作成します。(「**項目の場所を入力してください**」で BaseBack.cmd のパスを指定します。)
9. Sysprep ユーティリティーを実行します。
10. デプロイメントのイメージが作成されます。

各 PC にイメージが配信され、PC の個人情報設定を行った後、「**基本バックアップの作成**」アイコンをクリックすると、Rescue and Recovery が起動し、基本バックアップが作成することができます。

基本バックアップへの Sysprep イメージの取り込み

基本バックアップに Sysprep イメージを取り込むには、次のようにします。

1. 管理用インストールを実行します。SETUP_TVTRNRXXXX.EXE (ここで XXXX はビルド ID です) を一時フォルダーに展開します。

```
:: Extract the WWW EXE to the directory C:¥IBMRR
    start /WAIT setup_tvtrnrXXXX.exe /a /s /v"/qn TARGETDIR="C:¥TVTRR"" /w
```

2. C:¥TVTRR¥Program Files¥IBM ThinkVantage にある TVT.TXT ファイルの末尾に次のセクションを追加します。

```
[Backup0]
BackupVersion=2.0
```

3. MSIEXE ファイルを使用して Rescue and Recovery をインストールするには:
   a. MSI インストール時に以下のオプションをつけるとインストール時のログを作成することができます。

   ```
   /L*v %temp%¥rrinstall.txt
   ```

   b. MSIEXE ファイルを使用してインストールするには、次のコマンドを実行します。

   ```
   : Perform the install of Rescue and Recovery

    msiexec /i "C:¥TVTRR¥Rescue and Recovery - Client
   Security Solution.msi"
   ```

   c. MSIEXE を使用してサイレント・インストールを実行するには:

   最後に起動をする場合は、次のコマンドを実行します。

   ```
   : Silent install using the MSI with a reboot
   : Type the following command on one line

   start /WAIT msiexec /i "C:¥TVTRR¥Rescue and Recovery - Client
   Security Solution.msi" /qn
   ```

   注: 上記のコマンドはこのページに入るように修正されています。このコマンドを 1 行として入力してください。

   インストール後に再起動をしないようにするには、次のコマンドを実行します。

```
: Silent install using the MSI without a reboot
: Type the following command on one line

start /WAIT msiexec /i "C:¥TVTRR¥Rescue and Recovery - Client
Security Solution.msi" /qn REBOOT="R"
```

注: 上記のコマンドはこのページに入るように修正されています。このコマンドを 1 行として入力してください。

4. 次のコマンドを実行します。

```
:Start the Rescue and Recovery Service
net start  "TVT Backup Service"

:Create Sysprep Base Backup to Local Hard Drive
: Type the following command on one line

cd ¥"Program Files"¥"IBM ThinkVantage¥Rescue and Recovery"
rrcmd sysprepbackup location=l name=Sysprep Backup"
```

パスワードを使用する場合は、構文 password=*pass* を追加します。

5. 次のメッセージが表示されたら、Sysprep を実行します。

```
****************************************************
** Ready to take sysprep backup.                  **
** PLEASE RUN SYSPREP NOW AND SHUT DOWN.          **
**                                             **
** Next time the machine boots, it will boot      **
** to the PreDesktop Area and take a backup.      **
****************************************************
```

6. Sysprep が完了すると、PC がシャットダウンされますので、PC の電源を再度オンにします。

   注: オペレーティング・システムが再起動して、 Rescue and Recovery ワークスペースに入ります。「**システムの復元中**」というステータス・バーが表示されます。
7. 完了すると、「**The Sysprep Backup is Complete**」というメッセージが表示されます。
8. 「再始動」ボタンを押して再起動します。
9. デプロイメント用のイメージを取り込みます。

複数パーティションを持つ PC の取り込みと、Sysprep イメージ内のファイルを除外

Sysprep イメージで複数のパーティションを取り込むには、次のようにします。

1. 管理用インストールを実行します。SETUP_TVTRNRXXXX.EXE (ここで XXXX はビルド ID です) を一時フォルダーに展開します。

```
:: Extract the WWW EXE to the directory C:¥TVTRR
    start /WAIT setup_tvtrrXXXX.exe /a /s /v"/qn TARGETDIR="C:¥TVTRR"" /w
```

2. C:¥¥"tvtrr¥Program Files"¥"IBM ThinkVantage¥Rescue and Recovery" にある TVT.TXT ファイルの末尾に次のセクションを追加します。

```
[Backup0]
BackupVersion=2.0

[BackupDisk]
CustomPartitions=0
```

パーティションを除外するには、TVT.TXT ファイルに以下のセクションを追加します。

```
[BackupDisk]
CustomPartitions=1

[PartitionX].
IncludeInBackup=0
```

ここで、「**X**」は区画番号です。

3. バックアップから .MPG および JPG ファイルを除外するには、次の例のように IBMFILTER.TXT に追加します。

   ```
   X=*.JPG
   X=*.MPG
   ```

4. MSIEXE を使用して Rescue and Recovery をインストールするには:
   a. 以下のオプションをつけるとインストール時のログを作成することができます。

      ```
       /L*v %temp%¥rrinstall.txt
      ```

   b. MSIEXE を使用してインストールするには、次のコマンドを実行します。

      ```
      : Perform the install of Rescue and Recovery

       msiexec /i "C:¥TVTRR¥Rescue and Recovery - Client Security Solutiion.msi"
      ```

   c. MSIEXE を使用してサイレント・インストールするには:

      最後に起動をする場合は、次のコマンドを実行します。

      ```
      : Silent install using the MSI with a reboot

      : Type the following command on one line
      start /WAIT msiexec /i "C:¥TVTRR¥Rescue and Recovery - Client
      Security Solutiion.msi" /qn
      ```

      注: 上記のコマンドはこのページに入るように修正されています。このコマンドを 1 行として入力してください。

      インストール後に再起動しない場合は、次のコマンドを実行します。

      ```
      : Silent install using the MSI without a reboot

      : Type the following command on one line
      start /WAIT msiexec /i "C:¥TVTRR¥Rescue and Recovery -
      Client Security Solutiion.msi" /qn REBOOT="R"
      ```

      注: 上記のコマンドはこのページに入るように修正されています。このコマンドを 1 行として入力してください。

5. 次のコマンドを実行します。

   ```
   :Start the Rescue and Recovery Service
   net start  "TVT Backup Service"

   :Create Sysprep Base Backup to Local Hard Drive

   : Type the following command on one line
   cd ¥"Program Files"¥IBM ThinkVantage¥Rescue and Recovery"
   rrcmd sysprepbackup location=L name="Sysprep Base Backup"
   ```

   パスワードを使用する場合は、構文 password=*pass* を追加します。

6. 次のメッセージが表示されたら、Sysprep を実行します。

```
****************************************************
** Ready to take sysprep backup.                   **
** PLEASE RUN SYSPREP NOW AND SHUT DOWN.           **
**                                               **
** Next time the machine boots, it will boot       **
** to the PreDesktop Area and take a backup.       **
****************************************************
```

7. Sysprep が完了すると、PC がシャットダウンされますので、PC の電源を再度オンにします。

   注: オペレーティング・システムが再起動して、 Rescue and Recovery ワークスペースに入ります。「**システムの復元中**」というステータス・バーが表示されます。

8. 完了すると、「**The Sysprep Backup is Complete**」というメッセージが表示されます。
9. 「再始動」ボタンを押して再起動します。
10. デプロイメント用のイメージを取り込みます。

Windows 環境

バックアップに包含するファイルおよび除外するファイル

Rescue and Recovery には、バックアップ・ファイルの包含および除外の機能があります。個別のファイル、個別のフォルダー、または区画全体を包含および除外することができます。

以下に、包含および除外を設定するファイルをリストします。すべてのファイルは、C:¥program files¥ibm thinkvantage¥rescue and recovery フォルダーにあります。
1. IBMFILTER.TXT
2. GUIEXCLD.TXT

GUIEXCLD.TXT はデフォルトでは存在しません。GUI で包含および設定するファイルを指定すると作成されます。

デフォルトでは、エンド・ユーザーはバックアップから除外される個別のファイルおよびフォルダーを選択できます。このようなファイルおよびフォルダーは、ファイル GUIEXCLD.TXT に保存されます。

管理者が、特定のファイルまたはフォルダーが常にバックアップされるようにしたい場合、そのファイル名または種類を IBMIFILTER.TXT ファイルに含めることができます。このファイルの項目は、GUIEXCLD.TXT ファイル内の項目に関わらず、常にバックアップに含まれることになります。

また、管理者は、バックアップから常に除外するファイル、フォルダー、または区画を設定することもできます。

以下は、バックアップから常に除外されます。
- PAGEFILE.SYS
- HIBERFILE.SYS
- C:¥SYSTEM VOLUME INFORMATION

復元が行われる場合、PAGEFILE.SYS および HIBERFILE.SYS の両方は Windows により自動的に再生成されます。さらに、Windows の「システムの復元」データは、Windows により新規の復元ポイントを再生成します。

IBMFILTER.TXT

ファイル・フォーマットは、次のとおりです。

- 包含/除外につき 1 行の規則の入力。
- ファイルまたはフォルダーに複数の規則が適用される場合は、最後の規則が適用されます。ファイルの下部の入力が優先されます。
- 入力は、次のいずれかで記述する必要があります。
  - **;**

    は、コメント行です。
  - **I**

    は、その入力に一致するファイルまたはフォルダーがバックアップに包含されます。
  - **X**

    は、その入力に一致するファイルまたはフォルダーをバックアップから除外します。
  - **S**

    はファイルまたはフォルダー上に Single Instance Storage を包含します。
  - **i**

    は、包含するように選択することができるファイルまたはフォルダー用です。
  - **x**

    は、除外するように選択することができるファイルまたはフォルダー用です。
  - **s**

    はオプションで使用して、通常包含される Single Instance Storage としてファイルまたはフォルダーを識別します。

```
  S=*
  X=*
  i=*
I=*.ocx
I=*.dll
I=*.exe
I=*.ini
I=*.drv
I=*.com
I=*.sys
I=*.cpl
I=*.icm
I=*.lnk
I=*.hlp
I=*.cat
I=*.xml
I=*.jre
I=*.cab
I=*.sdb
```

```
I=*.bat
I=?:¥ntldr
I=?:¥peldr
I=?:¥bootlog.prv
I=?:¥bootlog.txt
I=?:¥bootsect.dos
I=?:¥WINNT¥*
I=?:¥WINDOWS¥*
X=?:¥WINDOWS¥prefetch¥*
I=?:¥minint¥*
I=?:¥preboot¥*
I=?:¥Application Data¥*
I=?:¥Documents and Settings¥*
I=?:¥IBMTOOLS¥*
I=?:¥Program Files¥*
I=?:¥msapps¥*
  X=?:¥Recycled
  X=?:¥RECYCLER
  x=?:¥Documents and Settings¥*¥Cookies¥*
x=?:¥Documents and Settings¥*¥Local Settings¥History¥*
X=?:¥Documents and Settings¥*¥Local Settings¥Temp¥*
x=?:¥Documents and Settings¥*¥Local Settings¥Temporary Internet Files¥*
x=?:¥Documents and Settings¥*¥Desktop¥*
x=?:¥Documents and Settings¥*¥My Documents¥*
  s=?:¥Documents and Settings¥*¥Desktop¥*
  s=?:¥Documents and Settings¥*¥My Documents¥*
  x=*.vol
  s=*.vol
```

Rescue and Recovery のその他の側面のカスタマイズ

インストール作業の前に定義された TVT.TXT という名前の外部ファイルを使用して Rescue and Recovery のさまざまな側面をカスタマイズできます。 TVT.TXT ファイルは、C:¥Program Files¥IBM ThinkVantage¥ サブフォルダー内にあります。

TVT.TXT ファイルは、Windows の INI ファイルのフォーマットに従い、データは [] で示されるセクションごとにまとめられ、以下の形式で 1 行に 1 つのデータが含まれています。

setting=*value*

たとえば、すべてのバックアップ・データを暗号化しない場合、TVT.TXT ファイルを以下のように設定します。

```
[Rescue and Recovery]

EncryptBackupData=0
```

EncryptBackupData に続く 0 パラメーターは、Rescue and Recovery にバックアップを暗号化しないように設定します。

TVT.TXT の [Rescue and Recovery] セクションの設定ストリング、パラメーター、およびデフォルト設定の全リストは、 157 ページの『付録 B. TVT.TXT の設定および値』に記載されています。

障害報告

現在、FTP や電子メールを介して Rescue and Recovery 環境から自動的に障害報告する方法はありません。エンド・ユーザーは、提出すべきファイルの場所に加えブラウザーに統合された電子メールの使用を指示されるでしょう。動的なデータの送信はサポートされていませんが、ロギング機能はログ・イベントをファイルにパッ

ケージして、電子メールで送信可能なパッケージ場所とファイル名のユーザーに送信します。これにより、*Req 115 障害報告票*の XML ファイルが作成されます。このファイルは「システム情報」に表示されるすべての情報 (現在のハードウェア、eGatherer、および PCDR 診断ログ情報) を組み合わせたもので、Rescue and Recovery 環境および OS - C:¥IBMSHARE の両方から容易にアクセス可能な場所に置かれます。

診断: は、ワークスペースで使用可能な基本アプリケーションであり、問題判別を支援します。これらのテストからの出力は、ヘルプ・デスクに表示または伝送できる方法で保存されます。Rescue and Recovery は、先にバックアップされたバージョンのユーザーの Windows 環境をリカバリーするためのツールを提供します。

Rescue and Recovery には、個別のファイルを復元するためのツールだけでなくユーザー区画を前のバージョンに完全に復元するためのツールも含まれています。ツールは、ユーザーのデータのバックアップへのアクセスを提供します。このデータの全部または一部をリカバリーする機能は、これらのツールによって提供されます。

OSFILTER.TXT

このファイルは、オペレーティング・システムおよびアプリケーションを、ユーザーのデータに影響を及ぼすことなくリカバリーします。Rescue and Recovery は、特定のファイルおよびフォルダー (サブフォルダーを含む) を、明示的な列挙およびワイルドカード・フィルターを使用することによって、他のデータを削除することなく、選択的に復元する機能を提供します。外部ファイルは、どのファイル、フォルダー、またはファイル・タイプ (ワイルドカードを利用) が OS およびアプリケーションを構成するか定義します。このファイルは管理者によってカスタマイズすることができ、デフォルトの外部ファイルが提供されます。ユーザーがオペレーティング・システムのリカバリーを選択すると、この外部ファイルに含まれている規則に一致するファイルのみ復元するオプションを選択可能なメニューが表示されます。管理者は、この外部ファイルの内容をカスタマイズできます。

OSFILTER.TXT ファイルを参照するには、このパスを使用します。`cd %RR%`。ファイル・フォーマットについては、20 ページの『IBMFILTER.TXT』を参照してください。

ワークスペース (Predesktop area)

Rescue and Recovery ワークスペース (PreDesktop Area) のうち、オペレーティング・システムが開かなくても開始される部分をカスタマイズするには、RRUTIL.exe ユーティリティー・プログラムを使用して、ファイルを抽出・適用します。これらのファイルおよびそれらのカスタマイズ・オプションは、次の表にリストされています。

表 1. RRUTIL.exe ファイルおよびカスタマイズ・オプション

ファイル/フォルダー	**カスタマイズ・オプション**
¥MININT¥SYSTEM32 WINBOM.INI	固定 IP アドレスの設定、画面の解像度の変更
¥MININT¥INF ¥MININT¥SYSTEM32¥DRIVERS	デバイス・ドライバーの追加

表 1. RRUTIL.exe ファイルおよびカスタマイズ・オプション (続き)

ファイル/フォルダー	カスタマイズ・オプション
MAINBK.BMP	Rescue and Recovery ワークスペース画面の背景の変更
MINIMAL_TOOLBAR(1).INI	アドレス・バーの無効化
NORM1.INI	Opera ブラウザーの設定、Opera アドレス・バーの無効化、Opera プロキシー設定の変更、修正ダウンロード・フォルダーの指定、ダウンロード可能なファイル・リストへの特定のファイル拡張子の追加、特定の拡張子を持つファイルの動作の変更
OPERA_010.CMD	Windows ユーザーのお気に入りの除外
OPERA6.INI	Opera ブラウザーの設定、アドレス・バーの無効化
PEACCESS*xx*.INI (ここで、*xx* は言語の指定です)	Rescue and Recovery ワークスペース内の GUI フォント、環境背景、左右パネルの項目と機能、HTML ベースのヘルプ・システムの設定
STANDARD_MENU.INI	「名前を付けて保存」ウィンドウの表示の有効化

RRUTIL.EXE の使用

RRUTIL.EXE および本書で言及するその他のユーティリティーは、本書が置かれている Web サイトから入手できます。

次の手順は、Rescue and Recovery ワークスペースからファイルを抽出し、そのファイルを適用する方法です。これらの手順は、Rescue and Recovery ワークスペースのすべてのファイル・カスタマイズで同じです。

RRUTIL.EXE を使用するには、次のようにします。
1. RRUTIL.exe を C ドライブのルートにコピーします。
2. GETLIST.TXT ファイルを次の構文で作成し、C:¥TEMP¥GETLIST.TXT として保存します。

   ```
   ¥preboot¥usrintfc¥file name
   ```

   ファイルを C:¥TEMP¥GETLIST.TXT として保存します。
3. コマンド・プロンプトで、RRUTIL.exe コマンド、および下表で定義されているいずれか 1 つのスイッチを入力します。その後、次の表に示されるような適切なパラメーターを指定してコマンドを入力します。

表 2. コマンドおよびスイッチ・オプション

コマンドおよびスイッチ・オプション	結果
`RRUTIL -l1`	preboot フォルダーの内容を表示する
`RRUTIL -l2`	minint フォルダーの内容を表示する
`RRUTIL -l4`	C ドライブのルートまたはタイプ 12 区画のルート (工場出荷時に Rescue and Recovery が Preload されているモデル (IBM_SERVICE 区画)) の内容を表示する
`RRUTIL -g C:¥temp¥getlist.txt C:¥temp`	Rescue and Recovery ワークスペース領域からファイルを取得する

表 2. コマンドおよびスイッチ・オプション (続き)

コマンドおよびスイッチ・オプション	結果
`RRUTIL -d C:¥temp¥ dellist.txt`	Rescue and Recovery ワークスペースからファイルを削除する
`RRUTIL -p C:¥temp`	Rescue and Recovery ワークスペースにファイルを追加または置換する
`RRUTIL -r` *path ¥oldname.ext newname.ext* `RRUTIL -r ¥temp¥rr¥test.txt test2.txt` ファイルは preboot¥rr フォルダー内にあります。	ワークスペースのファイルを名前変更する。
`RRUTIL -bp C:¥temp`	RRBACKUPS 仮想パーティションのファイルを更新または置換する。
`RRUTIL -bl` *path* RRUTIL -bl は `C:¥rr-list.txt` にリストする。 `rrutil -bl c:¥rrtemp`	RRBACKUPS フォルダーをリストする。
`RRUTIL -br RRbackups¥C¥n` ここで n はバックアップ数。	バックアップの内容を削除する
`RRUTIL -bg C:¥temp¥bgetlist.txt C:¥temp`	¥RRBACKUPS から個別ファイルをコピーする。
`RRUTIL -s`	RRBACKUPS が使用している容量を表示する。

4. ファイルを取得した後は、標準的なテキスト・エディターを使用してファイルを編集できます。

例: PEACCESSIBMxx.INI

この例は PEACCESSIBM*xx*.INI を参照しています。これは、Rescue and Recovery 環境のエレメントをカスタマイズできる設定ファイルです (26 ページの『Rescue and Recovery ワークスペースのカスタマイズ』を参照してください)。

注: ファイル名にある *xx* は、以下の 2 文字の言語省略語を表しています。

表 3. 言語コード

2 文字の言語コード	言語
br	ブラジル・ポルトガル語
dk	デンマーク語
en	英語
fi	フィンランド語
fr	フランス語
gr	ドイツ語
it	イタリア語
jp	日本語
kr	韓国語
nl	オランダ語
no	ノルウェー語
po	ポルトガル語
sc	中国語 (簡体字)
sp	スペイン語
sv	スウェーデン語
tc	中国語 (繁体字)

Rescue and Recovery ワークスペースからファイル PEACCESSIBMEN.INI の取得。

1. 次の行を含んだ GETLIST.TXT ファイルを作成します。
```
¥preboot¥reboot¥usrintfc¥PEAccessIBMen.ini
```
2. ファイルを C:¥TEMP¥GETLIST.TXT として保存します。
3. コマンド・プロンプトで、次のコマンドを実行します。
```
C:¥RRUTIL-g C:¥temp¥getlist.txt C:¥temp
```

ファイル PEACCESSIBMEN.INI を元の Rescue and Recovery ワークスペースに適用します。コマンド・プロンプトで、次のコマンドを実行します。

```
C:¥RRUTIL.EXE -p C:¥temp
```

注: 適用コマンド (**-p**) は、取得コマンド (**-g**) で作成されたフォルダー構造を使用します。編集したファイルを適切に配置するために、次の例のように、編集されたファイルが GETLIST.TXT ファイルで設定されているのと同じフォルダーに置かれていることを確認してください。

```
C:¥temp¥preboot¥usrintfc¥PEAccessIBMen.ini
```

例: ワークスペースへのデバイス・ドライバーの追加

1. デバイス・ドライバーをベンダーの Web サイトまたはその他のメディアから入手します。
2. 以下のフォルダーを作成します。
```
C:¥TEMP¥MININT¥INF
C:¥TEMP¥MININT¥SYSTEM32¥DRIVERS
```
3. ネットワーク・ドライバーの *.INF ファイルを MININT¥INF フォルダーにコピーします。 (たとえば、E100B325.INF は ¥MININT¥INF フォルダーに置く必要があります。)

4. *.SYS ファイルを ¥MININT¥SYSTEM32¥DRIVERS フォルダーにコピーします。 (たとえば、E100B325.SYS は MININT¥SYSTEM32¥DRIVERS フォルダーに置く必要があります。)
5. 関連する *.DLL、*.EXE、またはその他のファイルを ¥MININT¥SYSTEM32¥DRIVERS フォルダーにコピーします。(たとえば、E100B325.DIN または INTELNIC.DLL ファイルは、MININT¥SYSTEM32¥DRIVERS フォルダーに置く必要があります。)

   注:

   a. カタログ・ファイルは Rescue and Recovery ワークスペースで処理されないため、不要です。上記の手順は、PC を設定するために必要なすべてのデバイス・ドライバーにあてはまります。
   b. Rescue and Recovery ワークスペースの制限により、一部のアプリケーションまたは設定はレジストリーとして手動で行う必要があります。
6. デバイス・ドライバーを Rescue and Recovery ワークスペースに配置するには、コマンド・プロンプトから以下を実行します。

```
C:¥ RRUTIL.EXE -p C:¥temp
```

Rescue and Recovery ワークスペースのカスタマイズ

設定ファイル PEACCESSIBM*xx*.INI (ここで、*xx* は言語の指定です) を編集して、Rescue and Recovery 環境の以下のエレメントをカスタマイズできます。

- GUI フォント
- 環境背景
- Rescue and Recovery ワークスペースの左パネルにある項目および機能
- Rescue and Recovery ワークスペース内の HTML ベースのヘルプ

注: PEACCESSIBMEN.INI ファイルの取得、編集、および置換については、24 ページの『例: PEACCESSIBMxx.INI』を参照してください。

GUI フォントの変更

Rescue and Recovery ワークスペース上の GUI のフォントを変更することができます。デフォルト設定では、必要な言語および文字によって、すべてが正確に表示されない場合があります。初期設定は PEACCESSIBM*xx*.INI (ここで、*xx* は言語の指定です) の [Fonts] セクションに記述されています。以下は、日本語用の初期設定値です。

```
[Fonts]

LeftNavNorm = "MS UI Gothic"

LeftNavBold = "Arial Bold"

MenuBar = "MS UI Gothic"
```

以下のフォントは Rescue and Recovery ワークスペースと互換性があります。その他のフォントの互換性に関して IBM では動作確認をしておりません。

- Courier
- Times New Roman
- Comic Sans MS

Rescue and Recovery ワークスペースの背景の変更

右パネルの背景はビットマップ MAINBK.BMP で、¥PREBOOT¥USRINTFC フォルダーに置かれています。右パネルの背景用に独自のビットマップ・イメージを配置する場合、以下のサイズに準拠している必要があります。

- 幅 620 ピクセル
- 高さ 506 ピクセル

Rescue and Recovery で希望の背景を表示するには、ファイルを ¥PREBOOT¥USRINTFC フォルダーに置く必要があります。

注: MAINBK.BMP ファイルの取得、編集、および置換については、 23 ページの『RRUTIL.EXE の使用』を参照してください。

左パネルの項目および機能の変更

左パネルの項目を変更するには、PEACCESSIBM*xx*.INI (ここで、*xx* は言語の指定です) ファイルを編集する必要があります。Rescue and Recovery 環境から PEACCESSIBM*xx*.INI を取得して、ファイルを置換する方法については、 23 ページの『RRUTIL.EXE の使用』を参照してください。

Rescue and Recovery の左パネルには 21 の項目があります。各項目の機能は異なりますが、基本となる構文は同じです。以下に、左パネルの項目の例を示します。

```
[LeftMenu] button00=2, "Introduction", Introduction.bmp, 1,
1, 0, %sysdrive%¥Preboot¥Opera¥ENum3.exe,%sysdrive%¥Preboot¥Helps¥jp¥f_recovew.htm
```

表 4. 左パネルの項目およびカスタマイズ・オプション

項目	カスタマイズ・オプション
00-01	完全にカスタマイズ可能。
02	ボタン・タイプは 1 のままである必要がある (28 ページの表 5 を参照)。テキストは変更可能です。アプリケーションまたはヘルプ機能を定義できます。アイコンを追加することはできません。
03-06	完全にカスタマイズ可能。
07	ボタン・タイプは 1 のままである必要がある。テキストは変更可能です。アプリケーションまたはヘルプ機能を定義できます。アイコンを追加することはできません。
08-10	完全にカスタマイズ可能。
11	ボタン・タイプは 1 のままである必要がある。テキストは変更可能です。アプリケーションまたはヘルプ機能を定義できます。アイコンを追加することはできません。
16	ボタン・タイプは 1 のままである必要がある。テキストは変更可能です。アプリケーションまたはヘルプ機能を定義できます。アイコンを追加することはできません。
17-22	完全にカスタマイズ可能。

ボタン・タイプの定義: **`Button00`** の数字は他と重なってはいけません。若い数字の順で、左パネルに表示されます。

Button00=[0-8] このパラメーターでボタン・タイプを決定します。この値は、0 〜 8 まで指定できます。次の表に、各ボタン・タイプの値と動作が記載されています。

表 5. 項目タイプ・パラメーター

パラメーター	説明
0	空フィールド。この値は、行を空白または未使用のまま残す場合に使用します。
1	セクションの見出しテキスト。この設定は、主なグループまたはセクションの見出しを設定する場合に使用します。
2	アプリケーションの起動。ユーザーがボタンまたはテキストをクリックすると起動されるアプリケーションまたはコマンド・ファイルを定義します。
3	Rescue and Recovery ワークスペースの Opera ヘルプ。 Opera ブラウザーのヘルプ・トピックを定義します。
4	起動前に再起動メッセージ・ウィンドウを表示する。これらの値により、GUI は指定された機能を実行する前に PC を再起動する必要があるというメッセージをユーザーに表示します。
5	Lenovo Group Ltd に予約済み
6	Lenovo Group Ltd に予約済み
7	起動して待機します。この指定に続くフィールドは、Rescue and Recovery ワークスペースが続行する前に起動されたアプリケーションの戻り値を待つことを強制します。戻り値は、環境変数 %errorlevel% に返されます。
8	アプリケーションの起動。GUI はアプリケーションを起動する前に、国別コードと言語を検索します。CGI スクリプトを含む Web リンクが特定の国または特定の言語の Web ページを開くために使用されます。
9	Lenovo Group Ltd に予約済み
10	Lenovo Group Ltd に予約済み

入力フィールドの定義:

Button00=[0-10], "title"
: ボタン・タイプ・パラメーターに続くテキストにより、ボタンのテキストまたはタイトルが指定されます。テキストが左パネルの幅よりも大きい場合、テキストは切り取られ、省略符号ポイントによりさらに文字が続くことが示されます。吹き出しヘルプを使用しているときは、完全なタイトル・テキストが表示されます。

Button00=[0-10], "title", file.bmp
: タイトル・テキストの前に表示される前に表示されるアイコンとして使用するビットマップのファイル名を指定します。ビットマップのサイズは、15 ピクセル x 15 ピクセル以下でなければなりません。

Button00=[0-10], "title", file.bmp, [0 or 1]
: Rescue and Recovery ワークスペースで項目を表示するか、非表示にするかを設定します。値 `0` を設定すると、項目は非表示になり、空白行が表示されます。値 `1` を設定すると、項目は表示されます。

Button00=[0-10], "title", file.bmp, [0 or 1], 1
これは予約済みの機能であり、常に 1 に設定する必要があります。

Button00=[0-10], "title", file.bmp, [0 or 1], 1, [0 or 1]
項目を起動する前にパスワードを要求するには、1 を指定します。この値を 0 に設定すると、項目を起動する前にパスワードは要求されません。

Button00=[0-10], "title", file.bmp, [0 or 1], 1, [0 or 1], %sysdrive%[pathname¥executable]
%sysdrive% の値は、起動ドライブ名でなければなりません。起動ドライブ名の後に、アプリケーションまたはコマンド・ファイルの完全修飾パスを指定します。

Button00=[0-10], "title", file.bmp, [0 or 1], 1, [0 or 1],%sysdrive%[pathname¥executable], [parameters]
起動しているアプリケーションまたはコマンドに必要とされる任意のパラメーターを指定します。

これらのフィールドに値を指定しない場合、ボタンが正常に実行されるように、必要な数のコンマを入力する必要があります。たとえば、″Rescue and Recover″ というグループ見出しを作成する場合、以下のように指定します。

```
Button04=1, "Rescue and Recover",,,,,
```

項目 02、07、11 および 16 はタイプ 0 (または見出し) 項目のままにする必要があり、常にその数値的空間に整列しています。見出しの下に続く有効な項目の数を減らすには、完全にカスタマイズ可能な項目をタイプ 0、つまり左パネルの空白行に設定します。ただし、項目の総数は 23 を超えてはなりません。

下記の表はデフォルトで、左パネルの項目から起動できる機能および実行可能ファイルを示しています。

表 6. 左パネルの機能および実行可能ファイル

機能	実行可能ファイル
ファイルのレスキュー	WIZRR.EXE
システムの復元	WIZRR.EXE
移行ファイルの作成	WIZRR.EXE
ブラウザーを開く	OPERA.EXE
ネットワーク・ドライブの割り当て	MAPDRV.EXE
ハードウェアの診断	RDIAGS.CMD; PC Dr アプリケーションを起動します。IBM および Lenovo ブランドのプリインストール・モデルのみ
診断ディスクの作成	DDIAGS.CMD

右パネルの項目および機能の変更

右パネルの項目を変更するには、PEACCESSIBM*xx*.INI (ここで、*xx* は言語の指定です) ファイルを編集する必要があります。Rescue and Recovery 環境から PEACCESSIBM*xx*.INI を取得し、ファイルを置換するための詳細は、24 ページの『例: PEACCESSIBMxx.INI』を参照してください。

右パネルの機能リンクおよびユーザー・メッセージとウィンドウはカスタマイズ可能です。

右パネルの機能リンクのカスタマイズ: 右パネルの上部にあるリンクの機能を変更するには、PEACCESSIBM*xx*.INI (ここで、*xx* は言語の指定です) の [TitleBar] セクションを変更します。これらのリンクは、左パネルの項目と同じ方法で作動します。ボタン番号値は、00 から 04 です。左パネルと同じアプリケーションを [TitleBar] 項目から起動できます。タイトル・バーから開始できる実行可能ファイルの全リストは、23 ページの『RRUTIL.EXE の使用』を参照してください。

ユーザー・メッセージおよびウィンドウ状況の変更: PEACCESSIBM*xx*.INI (ここで、*xx* は言語の指定です) には、変更できるユーザーへのメッセージのある次の 2 つのセクションが含まれています。

```
[Welcome window]
```

```
[REBOOT]
```

「ようこそ」ウィンドウは、PEACCESSIBM*xx*.INI (ここで、*xx* は言語の指定です) の [Welcome] セクションで定義されています。左パネルに対する変更内容に応じて、タイトル行および 01 行目から 12 行目までの情報を変更できます。次のようにして、タイトル、見出し、および太字が表示されるフォントを設定できます。

```
[Welcome]
Title = "Rescue and Recovery へようこそ"
Line01 = "Rescue and Recovery(TM) ワークスペースには、Windows(R) 環境への
アクセスを妨げる問題からリカバリーするために役立つ、いくつものツールが
用意されています。"
Line02 = "以下の項目を実行できます。"
Line03 = "* Rescue and Recovery(TM) を使用してファイル、フォルダー、または
バックアップをレスキューおよび復元"
Line05 = "* システム設定およびパスワードを構成"
Line06 = "システム設定およびパスワード"
Line07 = "* インターネットを使用して通信し、Lenovo サポート・サイトにリンク"
Line08 = "インターネットを使用して、IBM サポート・サイトにリンク"
Line09 = "* 診断を使用して問題をトラブルシューティング"
Line10 = "診断を使用して問題を診断"
Line11 = "インストール・オプションに応じて機能は変わります。
詳しくは、「Rescue and Recovery」メニューで「概要」をクリックしてください。"
Line12 = "注:"
Line13 = "このソフトウェアをご使用いただくと、ご使用条件に合意いただいたことに
なります。ライセンスを表示するには、「Rescue and Recovery 」ツールバーで
「ヘルプ」をクリックし、さらに「ライセンスの表示」をクリックしてください。"
Continue = "続行"
NowShow = "再び表示しない"
NoShowCk =0
WelcomeTitle = "Arial Bold"
WelcomeText = "Arial"
WelcomeBold = "Arial Bold"
```

以下の設定値は、ユーザー・インターフェースにある「タイトル・バー・ヘルプ」機能用です。

Command0
: デフォルトで表示される HTML ベースのヘルプ・ページ

Command1
: Lenovo ご使用条件 HTML ページ

HELP ヘルプ

LICENSE
ライセンス

CANCEL
取り消し

Command0
%sysdrive%¥Preboot¥Helps¥jp¥f_welcom.htm

Command1
%sysdrive%¥Preboot¥Helps¥jp¥C_ILA.htm

「ようこそ」ウィンドウを表示しないようにするには、`NoShowCk = 0` を `NoShowCk = 1` に変更します。タイトルおよび内容の表示フォントを変更するには、セクションの最後の 3 行を編集します。

注: 行 14 および 15 は変更または削除しないでください。

PEACCESSIBM*xx*.INI (ここで、*xx* は言語の指定です) ファイルの [REBOOT] セクションで、以下の行の値を変更できます。

```
NoShowChk=
```

```
RebootText =
```

「NoShowChk」で指定できる値は `0` および `1` です。ユーザーが選択すれば、メッセージを隠すこともできます。メッセージが表示されるときにチェック・ボックスをクリックすると、値は `0` に設定されます。メッセージを表示するには、値を `1` に変更します。必要に応じて、[REBOOT] セクションのメッセージのフォントを変更できます。たとえば、次のようにして、この値を設定できます。

```
RebootText = "Arial"
```

注: PEACCESSIBM*xx*.INI (ここで、*xx* は言語の指定です) の [Messages]、[EXITMSG]、および [HelpDlg] セクションは、ファイルで表示できますが、カスタマイズできません。

Opera ブラウザーの設定

Opera ブラウザーには 2 つの設定ファイルがあります。1 つはデフォルト設定を含んでいます。もう 1 つは「アクティブな」設定です。エンド・ユーザーはアクティブ設定を変更することができますが、変更内容は Rescue and Recovery の再起動時に失われます。

ブラウザーの設定に永続的な変更を加えるには、OPERA6.INI と NORM1.INI の両方のコピーを編集します。これらのファイルは %systemdrive%、通常 C ドライブである C:¥PREBOOT¥OPERA¥PROFILE のフォルダー・パスにあります。OPERA6.INI の一時的な「アクティブ」コピーは RAM ドライブ (Z:) の Z:¥PREBOOT¥OPERA¥PROFILE フォルダーにあります。

注:

1. OPERA6.INI および NORM1.INI ファイルの取得、編集、および配置については、23 ページの『RRUTIL.EXE の使用』を参照してください。
2. Opera ブラウザーは、高度なセキュリティーを保つために一部のブラウザー機能が削除されています。

電子メール

Rescue and Recovery は Opera ブラウザーを介しての Web ベースの電子メールのサポートを提供します。また、大規模なエンタープライズ向けの設定を有効にすることができますが、IBM ではサポートしておりません。有効にする方法の参照情報を入手するには、「システム管理者のハンドブック (System Administrator's Handbook)」をお読みください。

http://www.opera.com/support/mastering/sysadmin/ (英語のサイトです。)

アドレス・バーの無効化

Opera のアドレス・バーを無効にするには、次の手順を実行します。

1. 23 ページの『RRUTIL.EXE の使用』で説明されている RRUTIL プロセスを使用して、MINIMAL_TOOLBAR(1).INI ファイルを C:¥PREBOOT¥OPERA¥PROFILE¥TOOLBAR から取得します。
2. ファイルを編集モードで開きます。
3. ファイルで [Document Toolbar] セクションを見付けます。
4. ″Address0″ 項目を見付けます。
5. ″Address0″ 項目の前にセミコロン (; コメント区切り記号) を入力します。

   注: ここで作業を終了してステップ 7 に進むと Opera ツールバーは無効になりますが、「移動」ボタンとツールバーが機能しないまま表示されています。「移動」ボタンとツールバーを削除するには、ステップ 6 に進んでください。
6. 次の項目を見付けて、それぞれの前にセミコロンを入力します。
   ```
   Button1, 21197=Go Zoom2
   ```
7. ファイルを保存します。
8. 23 ページの『RRUTIL.EXE の使用』に説明されているように、RRUTIL プロセスを使用してファイルを適用します。 Opera の実行時にアドレス・バーは無効になります。

ブックマークのカスタマイズ

Opera ブラウザーは、この RAM ドライブのファイル Z:¥OPERADEF6.ADR に展開されたブックマークを読み込むように設定されています。このファイルは、Rescue and Recovery の起動時に生成されます。起動時に、自動的に Windows Internet Explorer のブックマークがインポートされ、ブックマークが追加されます。起動時に生成される RAM ドライブのファイルは動的なファイルであるため、Windows 上でブックマークを Internet Explorer に追加すると、Rescue and Recovery ワークスペースの起動時にこれらの項目が自動的にインポートされます。

Internet Explorer のお気に入りの一部またはすべてを除外することができます。特定の Windows ユーザーのお気に入りを除外するには、次のようにします。

1. 23 ページの『RRUTIL.EXE の使用』に説明されているように、RRUTIL プロセスを使用して C:¥PREBOOT¥STARTUP¥OPERA_010.CMD を取得します。
2. ファイルを編集モードで開きます。
3. .CMD ファイルで PYTHON.EXE.FAVS.PYC Z:¥OPERADEF6.ADR という行を見付けます。

4. このコードの行末に、お気に入りを除外する Windows ユーザーの名前を引用符で囲んで入力します。たとえば、すべてのユーザーおよび管理者のお気に入りを除外する場合のコードは次のようになります。

```
python.exe favs.pyc z:¥Operadef6.adr "All Users, Administrator"
```

5. ファイルを保存します。
6. 23 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、ファイルを適用します。

すべての Windows ユーザーの Internet Explorer のお気に入りを Rescue and Recovery 環境で提供されるブラウザーで表示したくない場合、次のようにします。

1. 23 ページの『RRUTIL.EXE の使用』に説明されているように、RRUTIL プロセスを使用して編集するための C:¥PREBOOT¥STARTUP¥OPERA_010.CMD を取得します。
2. .CMD ファイルで PYTHON.EXE.FAVS.PYC Z:¥OPERADEF6.ADR という行を見付けます。
3. 以下のいずれかを実行します。
   a. 次のように、行頭に REM と入力します。

      ```
      REM python.exe favs.pyc z:¥Operadef6.adr
      ```

   b. ファイルからコードの行を削除する。
4. ファイルを保存します。
5. 23 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、ファイルを元に戻します。

プロキシー設定の変更

Opera ブラウザーのプロキシー設定を変更するには、次のようにします。

1. 23 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、編集のための C:¥PREBOOT¥OPERA¥PROFILE¥NORM1.INI ファイルを取得します。
2. NORM1.INI ファイルの最後に次のセクションを追加します。

   注: [0 or 1] の変数は、チェック項目が有効 (1) または無効 (0) であることを示しています。

   ```
   [Proxy]

   Use HTTPS=[0 or 1]

   Use FTP=[0 or 1]

   Use GOPHER=[0 or 1]

   Use WAIS=[0 or 1]

   HTTP Server=[HTTP server]

   HTTPS Server=[HTTPS server]

   FTP Server=[FTP server]

   Gopher Server= [Gopher server]

   WAIS Server Enable HTTP 1.1 for proxy=[0 or 1]

   Use HTTP=[0 or 1]
   Use Automatic Proxy Configuration= [0 or 1]
   Automatic Proxy Configuration URL= [URL]

   No Proxy Servers Check= [0 or 1]

   No Proxy Servers =<IP addresses>
   ```

3. ファイルを保存します。
4. 23 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、ファイルを元に戻します。

HTTP、HTTPS、FTP、Gopher、または WAIS プロキシーを追加するには、適切な行の後に `=<address of proxy>` と入力します。たとえば、プロキシー・サーバーのアドレスが http://www.your company.com/proxy である場合、HTTP サーバーの行は次のようになります。

```
HTTP Server=http://www.your company.com/proxy
```

項目にポートを追加する場合、アドレスの後にコロンを入力してから、ポート番号を入力します。″No Proxy Servers″ および ″Automatic Proxy Configuration URL″ も同様です。

```
z:¥preboot¥opera¥profile¥opera6.ini
```

ダウンロード先のパスの有効化または指定

「名前を付けて保存」ウィンドウを表示するには、いくつかの方法があります。ここでは、最も分かりやすい方法を説明します。

1. 23 ページの『RRUTIL.EXE の使用』で説明された RRUTIL プロセスを使用して、C:¥PREBOOT¥OPERA¥DEFAULTS¥STANDARD_MENU.INI ファイルを取得します。
2. `[Link Popup Menu]` セクションで、次の文字列を見付けます。
   ```
   ;;Item, 50761
   ```
3. 2 つのセミコロンを削除し、ファイルを保存します。Rescue and Recovery を再起動すると、エンド・ユーザーはリンクを右クリックでき、「リンク先を保存」オプションが表示されます。これで、「名前を付けて保存」ウィンドウが表示されるようになります。

   注: 直接のリンク (リダイレクトされるリンクではない) については、上記の手順で機能します。たとえば、リンクの対象が .PHP スクリプトである場合、Opera はスクリプトのみを保存し、スクリプトがポイントするファイルは保存しません。
4. 23 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、ファイルをフォルダー構造に戻します。

修正ダウンロード・フォルダーを指定するには、次のようにします。

1. 23 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、C:¥PREBOOT¥OPERA¥NORM1.INI ファイルを取得します。
2. ファイルで、次の行を見付けます。
   ```
   Download Directory=%OpShare%
   ```
3. `%OpShare%` を、ダウンロードするファイルを保存するフォルダーの絶対パスに変更します。
4. NORM1.INI ファイルを保存します。Rescue and Recovery ワークスペースを再起動すると、Opera はダウンロードされるファイルを指定されたフォルダーに保存することができるようになります。
5. 23 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、ファイルを元に戻します。

注:

1. ダウンロード先のパスをカスタマイズしても、リンクがリダイレクトされるファイルの場合はターゲット・ファイルを保存できません。
2. Opera ブラウザーは、.ZIP、.EXE、および .TXT ファイル・タイプのみをダウンロードするように設定され、これらのファイル・タイプについてのみ Opera の動作を変更します。 (3 文字のファイル拡張子を使用するファイルは数多くありますが、Rescue and Recovery ワークスペースが Windows 環境の代わりにならないのと同様、Opera ブラウザーもすべてのサービスを提供するブラウザーの代わりにはなりません。Rescue and Recovery ワークスペースでのインターネット・アクセスは、ユーザーの一時的なヘルプを目的として提供されていますので認識されるファイル・タイプの数を限定しています。ファイルのレスキューとシステムのリカバリーを行うためには、.ZIP、.EXE、.TXT ファイルでほとんど対応可能であるからです。別のファイルをダウンロードする必要がある場合、.ZIP ファイルを作成して、後で解凍してください。)
3. ファイル・タイプは、拡張子ではなく、MIME タイプで識別します。たとえば、.TXT ファイルに拡張子 .EUY の名前を付けても、このファイルは Opera ブラウザーでテキスト・ファイルとして開かれます。

ダウンロード可能なファイル拡張子の追加

Rescue and Recovery ブラウザーでダウンロードできるファイルの拡張子を追加することができます。追加するには、次の手順を実行します。

1. すべての Opera ウィンドウ (Rescue and Recovery ヘルプ・ファイルを含む) が閉じていることを確認します。
2. 23 ページの『RRUTIL.EXE の使用』内で説明された RRUTIL プロセスを使用して、C:¥PREBOOT¥OPERA¥NORM1.INI ファイルを取得します。
3. ファイルで `[File Types]` セクションを見付けます。
4. 検索機能を使用して、該当するファイル拡張子がリストされているかどうかを確認してから、以下のいずれかを実行します。
   - 拡張子はあるが、その拡張子のファイルが機能していない場合は、次のステップを実行します。
     a. 拡張子の後の値を 8 から 1 に変更します。 (値 8 は、ブラウザーから該当拡張子のダウンロードを無効にします。値 1 は、ブラウザーから該当拡張子のダウンロードを有効にします。)たとえば、下記のように変更します。

        ```
        video/mgpeg=8,,,,mpeg,mpg,mpe,m2v,m1v,mpa,|
        ```

        から

        ```
        video/mpeg=1,,,,mpeg,mpg,mpe,m2v,m1v,mpa,|
        ```

     b. NORM1.INI ファイルの [File Types Extension] セクションにあるファイルの MIME タイプを検索します。たとえば、VIDEO/MPEG=,8 を検索します。
     c. 値 ,8 を次のように変更します。

        ```
        %opshare%¥,2
        ```

        注: 指定された値がすでに設定されている場合は、値を変更しないでください。
     d. ファイルを保存してから、ファイルを OPERA6.INI にコピーし、Rescue and Recovery を再起動して変更内容を有効にします。

- 拡張子が存在せず、該当するタイプのファイル拡張子のダウンロードができない場合は、次のようにします。
  a. NORM1.INI の [File Types Extension] セクションで、temporary= を見付けます。たとえば、次のような項目です。

     temporary=1,,,,lwp,prz,mwp,mas,smc,dgm,|
  b. リストにファイル拡張子を追加します。たとえば、認識される拡張子として .CAB を追加する場合、次のように追加します。

     ```
     temporary=1,,,,lwp,prz,mwp,mas,smc,dgm,cab,|
     ```

     注: 末尾のコンマおよびパイプ記号は、この設定を機能させるために必要です。いずれかが省略されると、リスト内のすべてのファイル拡張子が無効になります。
  c. ファイルを C:¥TEMP¥ に保存します。
  d. ファイルを OPERA6.INI にコピーします。
  e. Rescue and Recovery ワークスペースを再始動して、変更内容を有効にします。

特定の拡張子を持つファイルの動作の変更

ファイルの動作を変更するには、NORM1.INI ファイルを置換します。ファイルの動作を拡張子ごとに変更するには、次のようにします。

1. ヘルプ・ファイルを含む、Opera およびすべてのアクティブな Opera ウィンドウを閉じます。
2. 23 ページの『RRUTIL.EXE の使用』で説明された RRUTIL プロセスを使用して、編集のための PREBOOT¥OPERA¥NORM1.INI ファイルを開きます。
3. ファイルで [File Types] セクションから、該当する拡張子を検索します。たとえば、.TXT ファイルを IBMSHARE フォルダーに保存したいとします。
4. 次の項目を検索します。TEXT/PLAIN=2,,,,TXT,|

   注: 値 2 は、ブラウザーに Opera でテキストとして表示するように設定するものです。値 1 は、ブラウザーにターゲット・ファイルを IBMSHARE フォルダーに保存するよう設定しています。
5. .TXT の例に続けて、この行を次のように変更します。

   ```
   TEXT/PLAIN=1,,,,TXT,|
   ```
6. 23 ページの『RRUTIL.EXE の使用』で説明されているように、RRUTIL プロセスを使用してファイルを保存し、元に戻します。
7. 変更内容が有効になるように、Rescue and Recovery ワークスペースを再始動します。

固定 IP アドレスの追加

固定 IP アドレスを設定するには、次のファイルを変更する必要があります。

1. 23 ページの『RRUTIL.EXE の使用』で説明された RRUTIL プロセスを使用して、¥MININT¥SYSTEM32 WINBOM.INI ファイルを取得します。
2. WINBOM.INI ファイルの `[PnPDriverUpdate]` の前に `[WinPE.Net]` セクションを追加します。次を参考にしてください。

   ```
   [Factory]

   WinBOMType=WinPE

   Reseal=No

   [WinPE]
   ```

```
Restart=No
[PnPDriverUpdate]
[PnPDrivers]
[NetCards]
[UpdateInis]
[FactoryRunOnce]
[Branding]
[AppPreInstall]
```

[WinPE.Net] セクションを作成し、以下の行を追加する必要があります。下記の設定はサンプルです。

```
[WinPE.Net]
Gateway=9.44.72.1
IPConfig =9.44.72.36
StartNet=Yes
SubnetMask=255.255.255.128
```

表 7. 固定 IP アドレス項目

項目	説明
Gateway	ゲートウェイの IP アドレスを指定します。デフォルト・ゲートウェイを設定すると、IP ルーティング・テーブルにデフォルトの経路が作成されます。 **構文:** Gateway = *xxx.xxx.xxx.xxx*
IPConfig	Rescue and Recovery ワークスペース起動時にネットワーク接続に使用する IP アドレスを指定します。 **構文:** IPConfig = *xxx.xxx.xxx.xxx*
StartNet	ネットワーク・サービスを開始するかどうかを指定します。 **構文:** StartNet = *Yes* | *No*
SubnetMask	サブネットマスクを 32 ビット値で指定します。 **構文:** SubnetMask = *xxx.xxx.xxx.xxx*

3. 23 ページの『RRUTIL.EXE の使用』で説明された RRUTIL プロセスを使用して、PREBOOT¥IBMWORK NETSTART.TBI ファイルを取得します。
4. 下記を、

   ```
   factory -minint
   ```

   から

   ```
   factory -winpe
   ```
5. 以下の行をコメント・アウトします。

   ```
   regsvr32 /s netcfgx.dll
   netcfg -v -winpe
   net start dhcp
   net start nla
   ```

6. 23 ページの『RRUTIL.EXE の使用』で説明された RRUTIL プロセスを使用して、¥IBMWORK NETSTART.TBI および ¥MININT¥SYSTEM32 WINBOM.INI ファイルを元に戻します。

画面の解像度の変更

Rescue and Recovery ワークスペースのデフォルトの解像度 (800 x 600 x 16 ビット) 設定を変更するには、次のようにします。

1. 23 ページの『RRUTIL.EXE の使用』で説明された RRUTIL プロセスを使用して、MININT¥SYSTEM32¥WINBOM.INI ファイルを取得します。
2. ファイル WINBOM.INI で、以下の項目を追加します。

   ```
   [ComputerSettings]
   DisplayResolution=800x600x16 or 1024x768x16
   ```

   `¥preboot¥ibmwork¥netstart.tbi` を開き、`factory -minint` を `factory -winpe` に変更します。

   Rescue and Recovery ワークスペースが起動すると、起動時に「出荷時プリインストール」というタイトルのウィンドウが表示されます。さらに、色の数が数万色から 256 色に減ります。
3. 23 ページの『RRUTIL.EXE の使用』で説明された RRUTIL プロセスを使用して、MININT¥SYSTEM32¥WINBOM.INI ファイルを元に戻します。

アプリケーションの開始

Rescue and Recovery Rescue and Recovery ワークスペース環境は、スクリプト、プログラム、またはカスタマイズされたプログラムをサポートする機能を持っています。これらのスクリプトまたはプログラムは、Rescue and Recovery Rescue and Recovery ワークスペース環境がメイン PE インターフェース・ページに到達する前に処理されます。

スクリプトまたはプログラムを配置するフォルダーは Preboot¥Startup です。このフォルダー内のスクリプトまたはプログラムは、英数字で処理されます。したがって、A.BAT と呼ばれるスクリプトは 1.EXE よりも前に処理されます。

このフォルダー内にスクリプトまたはプログラムを配置するには、次のようにします。

1. 次の Lenovo Rescue and Recovery 管理ツールのサイトから RRUTIL を取得します。

   http://www.lenovo.com/ThinkVantage (英語のサイトです。)
2. 一時フォルダーを作成します
3. ¥Temp フォルダー内で、以下のフォルダー・ツリーを作成します。
   ¥preboot¥startup
4. スクリプトまたはプログラムを ¥temp¥preboot¥startup パス内に配置します。
5. コマンド・ラインから RRUTIL 内に、-p ¥Temp を入力します
6. スクリプトまたはプログラムが正常にコピーされたことを検証するには、RRUTIL 内にコマンド・ラインから -g を入力します。これは、getlist.txt という名前のファイルを生成します。
7. ¥preboot¥startup フォルダーの getlist.txt の内容を調べます。スクリプトまたはプログラムはこのツリーの下にリストされているはずです。

パスワード

ワークスペースで使用可能なパスワード・オプションが 4 つあります。以下のとおりです。

- ワークスペースまたはマスター・パスワード
- ユーザー ID とパスワード、またはパスフレーズ
- バックアップ・パスワード
- パスワードなし

ワークスペースまたはマスター・パスワード

個別のワークスペース・パスワードを設定することができます。このパスワードはコマンド・ライン・インターフェースを介して設定でき、Client Security Solution がインストールされていない場合に、唯一使用可能なパスワード・オプションです。

このワークスペース・パスワードは、以下のコマンドを使用して作成できます。C:¥Program Files¥IBM ThinkVantage¥Client Security Solution¥pe_setupmasterpwde.exe.

このコマンドのパラメーターは以下のとおりです。

表 8.

パラメーター	説明
create password	このパラメーターは実際のパスワードを作成します。
verify password	このパラメーターは、パスワードが有効であり使用できることを確認します。
change currentPassword *newPassword*	このパラメーターによって、現在のパスワードを別のパスワードに変更することができます。
exists	このパラメーターは、パスワードが存在するかどうかを確認します。
サイレント	このパラメーターは、すべてのメッセージを非表示にします。
setmode values	0 = 認証は必要ありません。 1 = ユーザー固有の認証が必要です。 2 = マスター・パスワードが必要です。

注: 限定ユーザーはパスワードを変更できません。管理者は限定ユーザーに対してパスワードをリセットできます。

ユーザー ID とパスワード、またはパスフレーズ

このオプションは、パスワードまたはパスフレーズ管理に Client Security Solution コードを使用します。ワークスペースの始動時に、Client Security ログオンはユーザーに、このパスワードまたはパスフレーズに対するプロンプトを出します。これは、マルチユーザー環境により良いセキュリティーを提供します。ユーザーがログオンを使用してログオンする場合、そのユーザーはそのユーザーのファイルのみにアクセスが許可され、ほかのユーザーのファイルには許可されません。

このオプションは、CSS GUI によって、または XML スクリプトを介して設定できます。

バックアップ・パスワード

バックアップ・パスワードは、GUI 設定パスワードまたはコマンド・ライン・インターフェース rrcmd を介して、指定されたバックアップを使用して設定できます。以下に例を挙げます。

```
rrcmd backup location=L name=mybackup password=pass
rrcmd basebackup location=L name=basebackup password=pass
rrcmd sysprepbackup location=L name="Sysprep Backup" password=pass
```

パスワードなし

このオプションは認証を使用せず、ユーザーはパスワードを使用しないでワークスペースに入ることを許可されます。

ID パスワード・アクセス

パスワード・アクセスには 3 つのオプションがあります。

- マスター・パスワード
- ユーザー ID とパスワード、またはパスフレーズ
- パスワードなし

マスター・パスワード

マスター・パスワードは、ワークスペースおよびバックアップへのアクセスを許可する単一パスワードです。これはコマンド・ライン・インターフェースを介して設定され、Client Security Solution がインストールされていない場合、唯一のパスワード・オプションです。

ユーザー ID とパスワード、またはパスフレーズ

このオプションは、パスワードまたはパスフレーズ管理に Client Security Solution コードを使用します。ワークスペースの始動時に、Client Security Solution GINA はユーザーに、このパスワードまたはパスフレーズに対するプロンプトを出します。これは、マルチユーザー環境により良いセキュリティーを提供します。ユーザーが GINA を使用してログオンする場合、そのユーザーはそのユーザーのファイルのみにアクセスが許可され、ほかのユーザーのファイルには許可されません。

注: これにはまた、ユーザーの SecureDrive PrivateDisk の暗号化されたボリューム・ファイル内の情報も含まれています。

このオプションは、コマンド・ライン・インターフェースまたは GUI を介して設定できます。

パスワードなし

このオプションは認証を使用せず、ユーザーはパスワードを使用しないでワークスペースに入ることを許可されます。

復元タイプ

以下にファイルを復元するための方法を挙げます。

- ファイルのレスキュー
- 個別ファイルの復元
- オペレーティング・システムおよびアプリケーション
- システムの活性化
- 全体を復元
- 工場出荷時/Image Ultra ビルダー

注: Rescue and Recovery は、復元後にドメイン・ユーザーのキャッシュされたクレデンシャルを取り込むことはできません。

ファイルのレスキュー (すべての復元の前に)

この機能はユーザーに、バックアップ・ストレージの場所に対するプロンプトを出し、次にユーザーがバックアップを選択します。 ThinkVantage Rescue and Recovery は次に、ログインしたユーザーがアクセスを許可されているファイルを表示します。次にユーザーは、レスキューするファイルまたはフォルダー (あるいはその両方) を選択します。システムは、それからローカル HDD 以外の、ファイルをレスキューするために使用可能な場所を表示します。ユーザーは十分なスペースのある宛先を選択し、システムはそのファイルを復元します。

個別ファイルの復元

この機能はユーザーに、バックアップ・ストレージの場所に対するプロンプトを出し、次にユーザーがバックアップを選択します。 ThinkVantage Rescue and Recovery は次に、ログインしたユーザーがアクセスを許可されているファイルを表示します。次にユーザーは、レスキューするファイルまたはフォルダー (あるいはその両方) を選択し、システムは元の場所へ復元します。

オペレーティング・システムおよびアプリケーション

この機能はユーザーに、バックアップを選択するオプションを提供し、システムは osfilter.txt 内の規則によって定義されたファイルを削除します。次に選択されたバックアップから、OSFILTER.TXT によって定義されたファイルを復元します。また tvt.txt ファイル内には、プログラムを指定できるオプションがあって、復元前、または復元後に実行します。『TVT の設定および値』を参照してください。 157 ページの『付録 B. TVT.TXT の設定および値』

注:

1. オペレーティング・システムおよびアプリケーションは常時、パスワードの保存を使用します。
2. オペレーティング・システムおよびアプリケーションの復元は、CD/DVD バックアップからは使用できません。

カスタム・タスクを追加して、バックアップおよび復元の両方の前と後に実行することができます。バックアップおよび復元の設定の詳細については、 157 ページの『付録 B. TVT.TXT の設定および値』を参照してください。

システムの活性化

システムの活性化を選択すると、Rescue and Recovery プログラムは、新規の増分バックアップをとり、ハードディスクおよびバックアップをデフラグすることによって、システム・パフォーマンスを最適化します。次に選んだバックアップから、選択された設定とデータを復元します。システムの活性化操作は、現在の設定およびデータの保守中に、ウィルス、アドウェアおよびスパイウェアを削除する助けになります。この操作には多少時間がかかる場合があります。

システムの活性化には、次の手順を実行します。

1. Rescue and Recovery インターフェースから、「**バックアップからシステムを復元する**」アイコンをクリックします。「システムの復元」画面が表示されます。
2. 「システムの復元」画面で、「**システムを活性化します。**」を選択します。
3. 次の手順を実行することによってシステムの活性化を行うために使用する、ドライブとバックアップを選択します。
   a. 使用可能なドライブのドロップダウン・メニューから適切なドライブを選択します。選択したドライブ上でファイルをバックアップして、Rescue and Recovery インターフェースで表示します。
   b. システムの活性化のために使用するバックアップ・ファイルを選択します。
   c. 「**次へ**」をクリックします。
   d. 選択されたバックアップがシステムの活性化のために使用するものであることを確認し、「**次へ**」をクリックして復元処理を開始します。この操作中は PC を電源オフにしないように注意します。
   e. 「**OK** をクリックして先に進みます。進行状況表示バーが表示されます。この操作には多少時間がかかります。

カスタム・タスクを追加して、システムの活性化の前か後のいずれかに実行することができます。システムの活性化の設定については、 157 ページの『付録 B. TVT.TXT の設定および値』を参照してください。

注: 選択されたバックアップが作成されたあとでインストールまたはアンインストールされたアプリケーションは、正しく機能するように再度インストールする必要がある場合があります。
重要: バックアップ、復元、活性化、またはアーカイブ手順を開始する前に、システムが AC 電源に接続されていることを確認してください。これを行わないと、データ損失または取り返しの付かないシステム障害という結果になる場合があります。

全体を復元

この機能は、ローカル・ドライブ上のすべてのファイルを削除し、選択されたバックアップからファイルを復元します。パスワードの保存が選択された場合、使用可能な最新のパスワードが復元されます。

工場出荷時/Image Ultra ビルダー (IUB)

この機能は、ハードディスクを消去し、すべてのファクトリー・プリインストール・ソフトウェアを再インストールします。

パスワードの保存

次の表では、パスワードの保存を使用するかどうかを決定するための考慮事項を示します。

表 9. パスワードの保存の考慮事項

問題	パスワードの保存を使用した場合の影響
ユーザーが現行のアカウントおよびパスワードを使用して古いバックアップを復元し、Windows にログインする場合、「暗号化されたファイル・システム」のファイルおよびフォルダーを開くことができない。これらのファイルは元のアカウントおよびパスワードに対して暗号化されており、保持されるアカウントおよびパスワードに対しては暗号化されていないため。	• ユーザーは暗号化されたファイル・システムのデータを失う。 • 暗号化されたファイル・システムおよび「パスワードの保存」の併用は不可。
バックアップ作成後にユーザーを追加し、その後バックアップ時点に復元した場合、新規で作成したユーザーのユーザー・フォルダーおよびその中のファイル、Internet Explorer の「お気に入り」および「アプリケーション」データが存在しない。	• 「ユーザー ID 文書の設定」がなくなる。 • データ損失の可能性がある。
現行アカウントおよびパスワードでユーザーを削除すると、すべてのバックアップから削除したユーザーの認証情報が削除される。	• ユーザーはデータにアクセスできない。
管理者またはネットワーク管理者が、何人かの元の従業員のアクセスを削除して基本バックアップを復元し、システムをリセットして、全従業員の認証アカウントを削除するため基本バックアップを復元しても、「パスワードの保存」を使用すると従業員は従来通りアクセスできる。	• 「Microsoft ユーザー ID」のメンテナンス操作の推奨事項および推奨事項に違反している。

ローカルのハードディスクから復元する場合、パスワードの保存が選択されていると、現在のパスワードが使用されます。 USB またはネットワークから復元する場合は、最新のバックアップのパスワードが使用されます。

ハードウェア・パスワードのリセット

ハードウェア・パスワードのリセット環境は、Windows とは独立して実行され、これにより、忘れたパワーオンおよびハードディスクのパスワードのリセットが可能になります。登録時に作成している一連の質問に応答することによって、ID が確立されます。このセキュア環境は、パスワードを忘れてしまう前にできるだけ早く作成し、インストールし、登録することが賢明です。忘れたハードウェア・パスワードは、登録が完了するまでリセットできません。この回復メディアは、選択された ThinkCentre™ および ThinkPad PC 上でのみサポートされています。

この環境を作成しても、忘れた Windows パスワード、または Rescue and Recovery ワークスペースと関連したパスワードからのリカバリーの助けにはなりません。こ

の環境を作成することで、そこから忘れたハードウェア・パスワードのリセットが可能な始動デバイス・メニューへ、ブート可能なデバイスを追加します。パワーオン・パスワードに対してプロンプトが出されているときに F12 を押すことで、このメニューへアクセスします。

パスワード・デプロイメントのセットアップ関連した 3 つのステージがあります。

1. パッケージ・ビルド
2. パッケージ・デプロイメント
3. 登録

この手順を開始する前に、BIOS 内に管理者またはスーパーバイザー・パスワードを設定します。 BIOS 管理者またはスーパーバイザー・パスワード設定がない場合は、環境はセキュアにはなりません。パスワードのリセット・パッケージをデプロイしようとするすべてのシステムは、スーパーバイザー・パスワードを持っている必要があります。この手順を完了すると、パワーオン・パスワードとハードドライブ・パスワードが同じになります。この手順は、セキュアな環境を作成するタスクを完了する助けとなり、またセキュアな環境が作成されたあとで、忘れたパスワードをリセットする助けとなるように設計されています。

パッケージ・ビルド

セキュア環境を作成するには、次のようにします。

1. ハードウェア・パスワードのリセット・インストール・アプリケーションで、「セキュアな環境の作成」にマークを付けて、ハードウェア・パスワードのラジオ・ボタンをリセットします。
2. 「OK」をクリックします。「BIOS スーパーバイザー・パスワード」ウィンドウが開きます。
3. 「スーパーバイザー・パスワードの入力」フィールドで、管理者またはスーパーバイザー・パスワードを入力します。これは、ハードウェア設定を保護するために BIOS にあらかじめ持っている管理者またはスーパーバイザー・パスワードです。
4. 「OK」をクリックします。「鍵の作成」ウィンドウが開きます。
5. 鍵生成領域で、以下のいずれかを実行します。

   最初にこのセキュアな環境を作成するときに、新規の鍵を作成する必要があります。鍵は、ID を認証するために使用されるセキュリティー機能です。これに続くセキュアな環境を作成するための試みは、エクスポートを選択した場合に、最初の試みで作成したのと同じ鍵を使用するか、または異なる鍵を作成するか、いずれかのオプションを与えます。この環境を 1 つの PC のためだけに作成する場合は、新規の鍵を生成することが賢明でしょう。新規のセキュアな OS をビルドするたびに、鍵の生成を決定することができます。ただしこのオプションには、各 PC 上の登録手順を再実行することが必要です。同じ鍵が使用される場合は、登録が再実行される必要はありません。いくつかの PC のためにこの環境を作成する場合は、同じ鍵を使いたいと思うかもしれません。しかし、同じ鍵を使用する場合には、セキュアな場所にその鍵を保管することをお勧めします。

   鍵生成領域で、以下のいずれかを実行します。

- これが鍵を作成する最初の機会であり、この PC だけにセキュアな環境を作成しようとする場合は、「新規の鍵の生成」ラジオ・ボタンを作成します。
- これが鍵を作成する最初の機会であり、ほかの PC へデプロイ可能なセキュアな環境を作成したい場合は、「新規の鍵の生成」ラジオ・ボタンにマークを付けます。次に、「鍵をファイルにエクスポート」チェック・ボックスにマークを付けます。「ブラウズ」ボタンを使用して、鍵を保管する場所を定義します。
- すでに鍵が作成済みで、ほかの PC へデプロイ可能なセキュアな環境を作成したい場合は、「ファイルから鍵をインポート」ラジオ・ボタンにマークを付けます。「ブラウズ」ボタンを使用して、使用する鍵を配置する場所を定義します。上記のオプションには、作成された鍵が必要です。

ThinkPad、ThinkCentre、また言語ごと (たとえばフランス語、ドイツ語、日本語) にデプロイするとき、サポートされたシステムの各タイプごとにドナー・システムをセットアップします。その目的は、Rescue and Recovery 区画を基にしていて、システムごとに異なる可能性のある OS を保証することです。

6. インストール領域で、「ハードウェア・パスワードのリセットを作成したあとで自動的にインストールする」チェック・ボックスのチェック・マークを外します。
7. 「**OK**」をクリックします。
8. 「ハードウェア・パスワード機能はインストール・パッケージが実行されるまでこの PC 上で使用可能になりません」と知らせるダイアログ・ボックスに、「**OK**」をクリックします。

実行可能ファイルへのパスを検索するには、コマンド・ライン・プロンプトで cd %rr%¥rrcd¥passwordreset¥pwdreset.exe と入力します。

パッケージ・デプロイメント

会社の既存の配布メディアを使用して、作成されたパッケージをデプロイします。

登録

パスワードのリセットを登録するには、次のようにします。

1. pwdreset.exe を実行します
2. 「OK」をクリックして、PC を再起動します。PC は再起動して、BIOS パスワードを入力するようにプロンプトを出します。 BIOS パスワードを入力して、「**Enter**」をクリックします。PC はセキュアな環境内へ再起動し、「ハードウェア・パスワードのリセットへようこそ」ウィンドウが開きます。
3. これがセキュアな環境を作成する最初の機会であるか、または PC とハードディスクを再登録したい場合は、「**ハードウェアのリセットのセットアップ**」ラジオ・ボタンにマークを付けます。
4. 「**次へ**」をクリックします。「ハードディスクのセットアップ」ウィンドウが開きます。
5. PC のシリアル番号領域で、セットアップしたい PC の横にある「セットアップ」チェック・ボックスにマークを付けます。
6. 「**次へ**」をクリックします。「新規パワーオン・パスワードを入力」ウィンドウが開きます。

7. 「**新規パワーオン・パスワード**」フィールドで、使用するパワーオン・パスワードを入力します。すでにパワーオン・パスワードがある場合は、フィールド内に入力したものにリセットされます。さらに、ハードディスクのパスワードも同じパスワードに設定されます。
8. 「**次へ**」をクリックします。「セキュリティーの質問と応答の作成」ウィンドウが開きます。
9. 3 つの質問フィールドのそれぞれで、使用する質問を入力します。
10. 3 つの応答フィールドのそれぞれで、各質問に対する応答を入力します。パワーオン・パスワードを忘れてそれをリセットしようとするイベント内で、各応答を知っていることが必要です。
11. 「**次へ**」をクリックし、それから「**完了**」をクリックします。 PC は Windows 環境内で再起動します。

次に、ハードウェア・パスワードのリセット・インストーラのエラー・メッセージを挙げます。最初の 2 つは一般タイトルで、メッセージの残りの部分と組み合わせて使用されます。どちらの場合も、製品を再インストールすることをお勧めします。

- **IDS_STRING_ERR** ″エラー″
- **IDS_STRING_ERR_INT** ″内部エラー″
- **IDS_STRING_ERR_CMDLINE** ″入力されたコマンド・ライン・オプションは認識されませんでした。¥n¥nUsage: scinstall [/postenroll | /biosreset | /newplanar]″
- **IDS_STRING_ERR_NOTSUPPORTED**

  ハードウェア・パスワードのリセットはこの PC ではサポートされていません。
- **IDS_STRING_ERR_MEM**

  この PC には、ハードウェア・パスワードのリセット機能を実行するのに十分なメモリーがありません。
- **IDS_STRING_ERR_ENVAR**

  必須の環境変数が失われています。 Rescue and Recovery 3.0 (またはそれ以上) は、ハードウェア・パスワードのリセット機能を使用するためにインストールされている必要があります。
- **IDS_STRING_ERR_MISSINGDLL**

  必須の DLL が失われています。 Rescue and Recovery 3.0 (またはそれ以上) は、ハードウェア・パスワードのリセット機能を使用するためにインストールされている必要があります。
- **IDS_STRING_ERR_BIOSMAILBOX**

  ハードウェア・パスワードのリセットの機能をインストールするための BIOS の更新が失敗しました。 PC の電源を切ってから再起動し、ハードウェア・パスワードのリセットのインストールを再試行してください。
- **IDS_STRING_ERR_INSTALLRETRY**

この操作は正常に完了しませんでした。再度試行するには、PC の電源を切って再起動し、ハードウェア・パスワードのリセットのインストールを再度実行します。

- **IDS_STRING_ERR_INSTALLPUNT**

  この操作は正常に完了しませんでした。この問題のトラブルシューティングには、システム管理者に相談するか、または詳細について Rescue and Recovery 文書を参照してください。

第 4 章 Client Security Solution のカスタマイズ

この章では、TPM について Trusted Computing Group (TCG) によって定義された用語を使用します。これらの用語についての詳細説明は、次のサイトにあるリファレンスと定義を参照してください。

http://www.trustedcomputinggroup.org/ (英語のサイトです。)

エンベデッド・セキュリティー・チップ/TPM の利点

TPM は、 TPM を利用するソフトウェアにセキュリティー関連の機能を提供するために設計されたエンベデッド・セキュリティー・チップです。エンベデッド・セキュリティー・チップは、システムのマザーボードに搭載され、ハードウェア・バスを介して通信します。 TPM を導入しているシステムは、暗号鍵を作成して暗号化することができ、同じ TPM のみが暗号化を解除することができます。このプロセスは、しばしば鍵のラッピング と呼ばれ、鍵の開示を防止するのに役立ちます。 TPM を備えたシステムでは、マスター・ラッピング鍵は、ストレージ・ルート鍵 (SRK) と呼ばれ、 TPM 自体の内部に保管されるので、鍵の秘密 (private) 部分は決して公開されません。エンベデッド・セキュリティー・チップは、他のストレージ・キー、署名鍵、パスワード、およびデータの他の小ユニットも保管できます。しかし、TPM には記憶容量の制限があるので、 SRK はチップ外に記憶するその他の鍵の暗号化に使用されます。 SRK はエンベデッド・セキュリティー・チップに残されることは決してないので、保護ストレージの基本になっています。

TPM によって保護されたデータが必要になると、保護データはセキュアな組み込みハードウェア環境に処理のために渡されます。認証と暗号化解除が正常に行われた後、無保護のデータはそのシステム内で使用することができます。

TPM を導入したシステムは、ハードウェアがソフトウェアよりも攻撃に強いのと同様に、攻撃に強くなります。これは、暗号鍵を利用するときに特に重要です。非対称鍵ペアの秘密 (private) の部分は、オペレーティング・システムが管理する記憶域から分離されて保持されます。 TPM は、独自の内蔵ファームウェアと論理回路を使用して命令を処理し、オペレーティング・システムには依存せず、外部ソフトウェアのぜい弱性に影響されません。

TPM 技術を使用しているシステムも含めて、完璧なセキュリティーを提供できるシステムはありません。エンベデッド・セキュリティー・チップは、改ざんやデータの解析が行われないように設計されています。 TPM に保護された機密事項を暴くために必要なこの種の解析を実行するには、PC に物理的にアクセスできることと、特殊な追加ハードウェアを必要とするために、エンベデッド・セキュリティー・チップが有効になっているプラットフォーム上の機密事項は、ソフトウェアのみのシステムよりも一層セキュアです。システムから機密事項を盗むことを困難にすることは、個人または企業のセキュリティーの全体レベルを上げることに役立ちます。

エンベデッド・セキュリティー・チップの使用は、オプションのプロセスで、Client Security Solution 管理者を必要とします。個人ユーザーでも企業の IT 部門で

も、 TPM は初期設定する必要があります。ハードディスク故障からのリカバリーやシステム・ボードの交換など、その後の操作は、Client Security Solution 管理者に限定されます。

Client Security Solution の暗号鍵の管理法

Client Security Solution の内部作業は、2 つの主なデプロイメント・アクティビティーである、『所有権の取得』と『ユーザー登録』で説明します。 Client Security セットアップ・ウィザードを初めて実行する際に、所有権の取得プロセスとユーザー登録プロセスが、どちらも初期設定時に実行されます。 Client Security セットアップ・ウィザードを完了した特定の Windows ユーザー ID は、Client Security Solution 管理者で、アクティブ・ユーザーとして登録されます。システムにログインするその他のユーザーは、すべて Client Security Solution に登録するように自動的に要求されます。

- **所有権の取得 - Client Security Solution 管理者を割り当てる**

  単一の Windows 管理者のユーザー ID は、唯一の Client Security Solution 管理者としてシステムに割り当てられます。 Client Security Solution の管理機能は、このユーザー ID により実行される必要があります。 TPM の許可は、このユーザーの Windows パスワードか、Client Security パスフレーズのいずれかです。

  注: 忘れてしまった Client Security Solution 管理者パスワードまたはパスフレーズからリカバリーする唯一の方法は、有効な Windows のアクセス権を使用してこのソフトウェアをアンインストールするか、 BIOS 内のセキュリティー・チップをクリアするかのいずれかです。いずれの方法でも、TPM に関連した鍵を介して保護されたデータは、消失します。 Client Security Solution は、忘れてしまったパスワードまたはパスフレーズの自分でリカバリーできるオプション機構も提供します。このため、パスワードまたはパスフレーズは、ユーザー登録機能の一部であるユーザー確認のための質問への応答を基にしています。 Client Security Solution 管理者は、この機能を使用するかしないかを決定します。

- **ユーザー登録**

  所有権の取得プロセスが完了し、 Client Security Solution 管理者が作成されると、ユーザー・ベース鍵 (User Base Key) を作成して、現在ログオンしている Windows ユーザーの信用証明情報を安全に保管することができます。この設計により、複数のユーザーが Client Security Solution に登録し、単一の TPM を利用することができます。ユーザー鍵は、セキュリティー・チップを介して保護されますが、実際にはチップ外のハードディスクに保管されます。他のセキュリティー・テクノロジーとは異なり、この設計では、セキュリティー・チップに構築された実際のメモリーの代わりに、制限のあるストレージ要素としてハードディスク・スペースを作成します。この設計により、同じセキュア・ハードウェアを利用できるユーザーの数が飛躍的に増大します。

所有権の取得

Client Security Solution のトラステッド・ルートは、システム・ルート・キー (SRK) です。この移動できない非対称鍵は、 TPM のセキュア環境内に生成され、システムに公開されることは決してありません。この鍵を利用する許可は、Windows 管理者アカウントにより「TPM_TakeOwnership」コマンドの実行中に得られます。

Client Security パスフレーズを利用している場合、 Client Security Solution 管理者の Client Security パスフレーズは、TPM 許可になり、それ以外の場合は Client Security Solution 管理者の Windows パスワードになります。

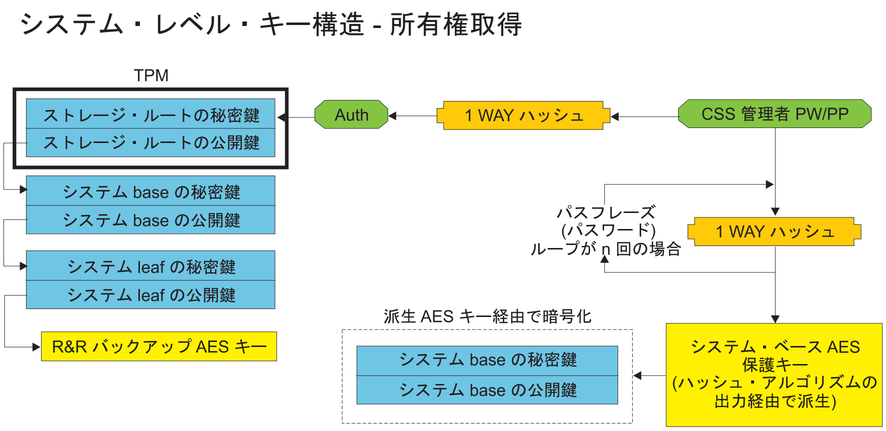


図 *1.*

システム用に作成された SRK では、その他の鍵ペアは、作成して TPM の外部に保管できますが、ハードウェア・ベースの鍵によってラップまたは保護されます。TPM は SRK を内蔵するハードウェアであり、ハードウェアは損傷することがあるので、システムへの損傷によりデータ・リカバリーが妨げられないようにするためにリカバリー機構が必要です。

システムをリカバリーするために、システム・ベース鍵 (System Base Key) が作成されます。この移動可能な非対称ストレージ・キーにより、 Client Security Solution 管理者は、システム・ボード交換や別システムへの計画的移行からリカバリーすることができます。

システム・ベース鍵を保護しながら、通常の操作またはリカバリー時にアクセスできるようにするために、このキーの 2 つのインスタンスが作成され、異なる 2 つの方法によって保護されます。最初に、システム・ベース鍵は、AES 対称鍵を使用して暗号化されます。この鍵は、Client Security Solution 管理者のパスワードまたは Client Security パスフレーズを知っていれば得ることができます。 Client Security Solution リカバリー・キーのこのコピーは、クリアされた TPM またはハードウェア障害により交換されたシステム・ボードからのリカバリー専用です。

Client Security Solution リカバリー・キーの 2 番目のインスタンスは、 SRK によってラップされてキー階層にインポートされます。システム・ベース鍵のこの 2 つのインスタンスにより、 TPM は自身にバインドされた秘密を通常の使用状態で保護することができ、さらに AES 鍵を使用して暗号化されているシステム・ベース鍵を介して、障害のあるシステム・ボードをリカバリーすることができます。AES 鍵は、 Client Security Solution 管理者パスワードまたは Client Security パスフレーズによってアンロックされます。

次に、システム・リーフ鍵 (System Leaf Key) が作成されます。このレガシー・キーは、バックアップを保護する Rescue and Recovery が使用した AES 鍵など、システム・レベルの機密事項を保護するために作成されます。

ユーザー登録

各ユーザーのデータを同じ TPM によって保護するために、各ユーザーは独自のユーザー・ベース鍵を作成します。この移動可能な非対称ストレージ・キーは、 2 回作成され、各ユーザーの Windows パスワードまたは Client Security パスフレーズから生成された対称 AES 鍵によって保護されます。次に、ユーザー・ベース鍵の 2 番目のインスタンスは、 TPM にインポートされ、システム SRK によって保護されます。図 2 を参照してください。

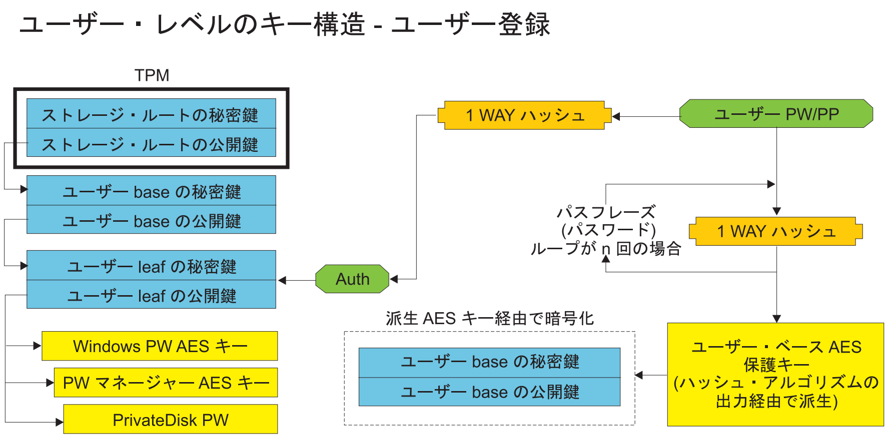


図 2.

作成されたユーザー・ベース鍵では、ユーザー・リーフ鍵 (User Leaf Key) と呼ばれる第 2 非対称鍵が、インターネット・ログオン情報の保護に使用される Password Manager AES 鍵、データの保護に使用される PrivateDisk パスワード、オペレーティング・システムへのアクセスを防護する Windows パスワード AES 鍵など、個別の秘密を保護するために作成されます。ユーザー・リーフ鍵へのアクセスは、ユーザーの Windows パスワードまたは Client Security Solution パスフレーズによって制御され、ログオン時には自動的にアンロックされます。

ソフトウェア・エミュレーション

システムに TPM が搭載されていない場合は、ソフトウェアをベースにしたトラステッド・ルートが使用されます。ユーザーは同じ機能を使用可能ですが、トラステッド・ルートはソフトウェア・ベースの鍵であるので、セキュリティーは低下します。 TPM の SRK は、 TPM が提供した保護を行うために、ソフトウェア・ベースの RSA 鍵と AES 鍵で置き換えられます。 RSA 鍵は AES 鍵をラップし、 AES 鍵は階層内の次の RSA 鍵の暗号化に使用されます。

システム・ボードの交換

システム・ボードを交換するということは、鍵がバインドされていた旧 SRK がもはや無効になり、別の SRK が必要とされていることが推測されます。これは TPM が BIOS によりクリアされても起こります。

Client Security Solution 管理者は、システムの信用証明情報を新規 SRK にバインドすることを要求されます。システム・ベース鍵は、 Client Security Solution 管理者の許可証明書から得たシステム・ベース AES 保護鍵により暗号化を解除する必要があります。 53 ページの図 3 を参照してください。

注: Client Security Solution 管理者がドメイン・ユーザー ID であり、そのユーザー ID のパスワードが別の PC 上で変更されていた場合、リカバリーを必要とするシステムにログオンするときに最後に使用されたパスワードが、リカバリーのためにシステム・ベース鍵の暗号化を解除するために既知である必要があります。たとえば、デプロイメント中に、 Client Security Solution 管理者のユーザー ID とパスワードが構成されており、このユーザーのパスワードが別の PC 上で変更されている場合は、デプロイメント中に設定された元のパスワードは、このシステムをリカバリーするための必須権限になります。

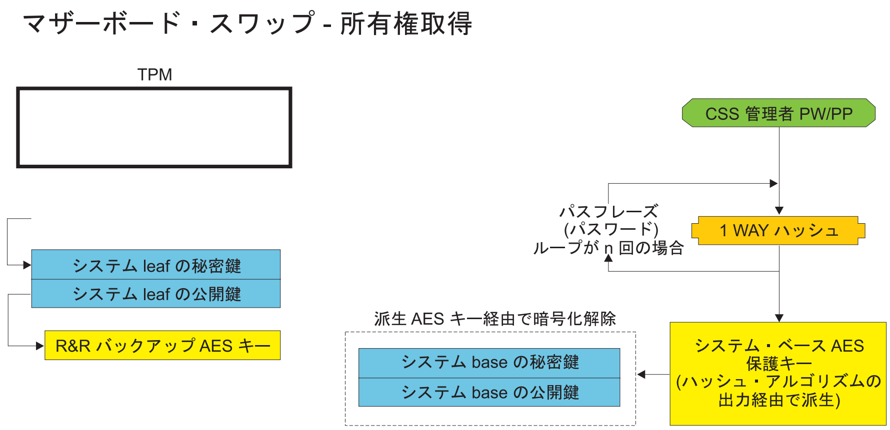


図 3.

以下のステップに従って、システム・ボードの交換を実施してください。

1. Client Security Solution 管理者は、オペレーティング・システムにログオンする
2. ログオン実行コード (cssplanarswap.exe) は、セキュリティー・チップが使用不可になっていることを認識し、使用可能にするために再起動を要求する (このステップは、BIOS によりセキュリティー・チップを使用可能にすることで回避できます)。
3. システムが再起動され、セキュリティー・チップが使用可能になる。
4. Client Security Solution 管理者がログオンし、次に、新規 Take Ownership プロセスが完了する。
5. システム・ベース鍵は、 Client Security Solution 管理者の認証によって得られるシステム基本 AES 保護鍵を使用して暗号化を解除される。システム・ベース鍵は、新規 SRK にインポートされて、システム・リーフ鍵とそれによって保護されているすべての信用証明情報を再設定します。
6. これで、システムはリカバリーされます。

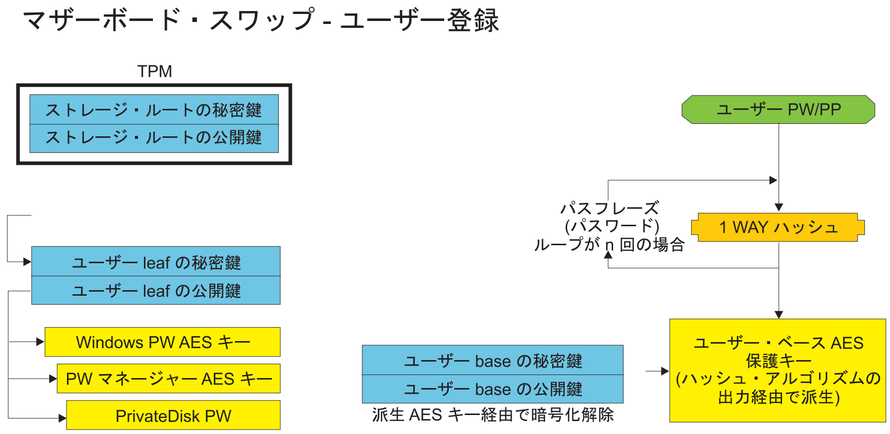


図 4.

各ユーザーがシステムにログオンする度に、ユーザー・ベース鍵がユーザー認証から得られるユーザー・ベース AES 保護鍵により自動的に暗号化を解除され、Client Security Solution 管理者により作成された新規 SRK にインポートされます。

XML スキーマ

XML スクリプト記述の目的は、IT 管理者が Client Security Solution のデプロイに使用できるカスタム・スクリプトを作成できるようにすることです。 Client Security Solution セットアップ・ウィザードで使用できるすべての機能は、スクリプト記述でも使用可能です。スクリプトは xml_crypt_tool 実行可能モジュールによって保護できます (パスワード (AES 暗号化) を使用または隠ぺいを行う)。いったん作成されると、仮想 PC (vmserver.exe) は、入力としてスクリプトを受け入れます。仮想 PC は、セットアップ・ウィザードと同一のファンクションを呼び出して、ソフトウェアを構成します。

使用法

すべてのスクリプトは、XML エンコード・タイプ、XML スキーマ、および実行する 1 つ以上の機能を指定する 1 つのタグより構成されています。スキーマは、XML ファイルを検証し、必須パラメーターがそろっていることを確認するために使用されます。スキーマの使用は、現在、推奨されていません。各ファンクションは、ファンクション・タグで囲まれています。各ファンクションには ORDER が含まれています。これは、コマンドが仮想 PC (vmserver.exe) によって実行される順番を指定します。各ファンクションには、バージョン番号も含まれます。現在、すべてのファンクションはバージョン 1.0 です。分かりやすくするために、以下のスクリプト例には、それぞれ 1 つのファンクションのみが含まれています。しかし、実際のスクリプトには複数のファンクションが含まれる可能性が高くなります。Client Security Solutions セットアップ・ウィザードを使用すれば、このようなスクリプトを作成できます。 176 ページの『Client Security ウィザード』を参照してください (詳細は、セットアップ・ウィザードの文書を参照してください)。

注: ドメイン名を必要とするファンクションのいずれかに、パラメーター <DOMAIN_NAME_PARAMETER> が残されている場合は、システムのデフォルトの PC 名が使用されます。

例

AUTO_ENROLL_ADMIN_FOR_RNR_ONLY

このコマンドにより、システム管理者は、 Rescue and Recovery を使用したバックアップの暗号化に必要なセキュリティー・キーを生成することができます。このコマンドは、システムごとに 1 回のみ実行してください。各ユーザーではなく、管理者のみが実行してください。

注: Rescue and Recovery のみがインストールされている場合、バックアップを TPM により暗号化するときは、管理者は TPM 所有者として割り当てられる必要があります。以下のスクリプト・ファイルを使用すると、管理者のユーザー ID とパスワードが自動的に割り当てられます。この Windows のユーザー ID とパスワードは、TPM のリカバリーのために使用されます。 (CSS XML スクリプト・ファンクション以外のものはすべて、 Rescue and Recovery のみがインストールされている場合は適用されません。)

- **USER_NAME_PARAMETER**

  管理者ユーザーの Windows ユーザー ID
- **DOMAIN_NAME_PARAMETER**

  管理者ユーザーのドメイン名
- **RNR_ONLY_PASSWORD**

  管理者ユーザーの Windows パスワード

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>AUTO_ENROLL_ADMIN_FOR_RNR_ONLY</COMMAND>
          <VERSION>1.0</VERSION>
          <USER_NAME_PARAMETER>WinAdminName</USER_NAME_PARAMETER
          <DOMAIN_NAME_PARAMETER>MyCorp</DOMAIN_NAME_PARAMETER>
          <RNR_ONLY_PASSWORD>WinPassw0rd<RNR_ONLY_PASSWORD>
         </FUNCTION>
</CSSFile>
```

ENABLE_TPM_FUNCTION

このコマンドは、TPM を使用可能にし、引数 SYSTEM_PAP を使用します。システムに既に BIOS Administrator/Supervisor パスワードが設定されている場合は、この引数を指定する必要があります。それ以外の場合、このコマンドはオプションです。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_TPM_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

DISABLE_TPM_FUNCTION

このコマンドは引数 SYSTEM_PAP を使用します。システムに既に BIOS Administrator/Supervisor パスワードが設定されている場合は、この引数を指定する必要があります。それ以外の場合、このコマンドはオプションです。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>DISABLE_TPM_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>password</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

ENABLE_ENCRYPT_BACKUPS_FUNCTION

Rescue and Recovery を使用するときは、このコマンドは Client Security Solution を使用したバックアップの保護を使用可能にします。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_ENCRYPT_BACKUPS_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

DISABLE_ENCRYPT_BACKUPS_FUNCTION

Rescue and Recovery を使用してバックアップを保護するときは、このコマンドは Client Security Solution を使用したバックアップの保護を使用不可にします。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>DISABLE_ENCRYPT_BACKUPS_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_PWMGR_FUNCTION

このコマンドは、すべての Client Security Solution ユーザーに対して Password Manager を使用可能にします。

```
 <?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_PWMGR_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_CSS_GINA_FUNCTION

このコマンドは、Client Security Solution のログオンを使用可能にします。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
```

```
          <COMMAND>ENABLE_CSS_GINA_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_UPEK_GINA_FUNCTION

ThinkVantage 指紋認証ユーティリティーがインストール済みの場合は、このコマンドはログオンを使用可能にします。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_UPEK_GINA_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_UPEK_GINA_WITH_FUS_FUNCTION

ThinkVantage 指紋認証ユーティリティーがインストール済みの場合は、ユーザーの簡易切り替え対応のログオンを使用可能にします。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_UPEK_GINA_WIH_FUS_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_NONE_GINA_FUNCTION

ThinkVantage 指紋認証ユーティリティーまたは Client Security Solution のいずれかのログオンが使用可能な場合は、このコマンドは ThinkVantage 指紋認証ユーティリティーと Client Security Solution の両方のログオンを使用不可にします。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_CSS_NONE_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

SET_PP_FLAG_FUNCTION

このコマンドは、Client Security パスフレーズを使用するか、 Windows パスワードを使用するかを決めるために、 Client Security Solution が読み取るフラグを書き込みます。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>SET_PP_FLAG_FUNCTION</COMMAND>
         <PP_FLAG_SETTING_PARAMETER>USE_CSS_PP</PP_FLAG_SETTING_PARAMETER>
         <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_PRIVATEDISK_PROTECTION_FUNCTION

このコマンドは、SafeGuard PrivateDisk をシステムで使用可能にします。 Safeguard PrivateDisk を使用するためには、各ユーザーを、 ENABLE_PD_USER_FUNCTION によって個別にセットアップする必要があります。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_PRIVATEDISK_PROTECTION_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

SET_ADMIN_USER_FUNCTION

このコマンドは、Client Security Solution の管理者ユーザーを決めるために Client Security Solution が読み取るフラグを書き込みます。パラメーターは次のとおりです。

- **USER_NAME_PARAMETER**

  Admin ユーザーのユーザー名
- **DOMAIN_NAME_PARAMETER**

  Admin ユーザーのドメイン名

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>SET_ADMIN_USER_FUNCTION</COMMAND>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

ENABLE_PD_USER_FUNCTION

このコマンドは、特定のユーザーが PrivateDisk を使用できるようにします。パラメーターは次のとおりです。

- **USER_NAME_PARAMETER**

  PrivateDisk を使用可能にするユーザーのユーザー名
- **DOMAIN_NAME_PARAMETER**

  PrivateDisk を使用可能にするユーザーのドメイン名
- **PD_VOLUME_SIZE_PARAMETER**

  PrivateDisk ボリュームのサイズ (MB)
- **PD_VOLUME_PATH_PARAMETER**

  作成する PrivateDisk ボリュームのパス
- **PD_VOLUME_NAME_PARAMETER**

作成する PrivateDisk ボリュームの名前。値 PD_USE_DEFAULT_OPTION が指定されている場合は、デフォルト値が自動的に使用されます。

- **PD_VOLUME_DRIVE_LETTER_PARAMETER**

  作成する PrivateDisk ボリュームのドライブ名。値 PD_USE_DEFAULT_OPTION が指定されている場合は、デフォルト値が自動的に使用されます。

- **PD_VOLUME_CERT_PARAMETER**

  値 PD_USE_CSS_CERT が渡されると、 PrivateDisk は新規証明書を作成するか、既存の証明書を使用して、それを Client Security Solution CSP で保護するかのいずれかを行います。このボリュームのマウント/アンマウントは、 CSS パスフレーズ/Windows パスワードの代わりに CSP に結合されます。値 PD_USE_DEFAULT_OPTION が指定されている場合は、証明書は使用されず、デフォルトである、ユーザーの CSS パスフレーズ/Windows パスワードが使用されます。

- **PD_USER_PASSWORD**

  PrivateDisk ボリュームをマウント/作成するために、 Client Security Solution が PrivateDisk を渡すパスワード。値 PD_RANDOM_VOLUME_PWD が指定されている場合は、 Client Security Solution は無作為のボリューム・パスワードを生成します。

- **PD_VOLUME_USER_PASSWORD_PARAMETER**

  PrivateDisk ボリュームをマウントするためのユーザー固有のパスワード。このパスワードは、PD_USER_PASSWORD パスワードへのバックアップ用です。何かの理由で将来 Client Security Solution が失敗した場合、この引数に対して渡された値は Client Security Solution から独立しています。値 PD_USE_DEFAULT_OPTION が指定されている場合は、値は使用されません。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_PD_USER_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <PD_VOLUME_SIZE_PARAMETER>500</PD_VOLUME_SIZE_PARAMETER>
          <PD_VOLUME_PATH_PARAMETER>C:¥Documents and Settings¥sabedi¥My Documents¥
             </PD_VOLUME_PATH_PARAMETER>
          <PD_VOLUME_NAME_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_NAME_PARAMETER>
          <PD_VOLUME_DRIVE_LETTER_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_DRIVE
             _LETTER_PARAMETER>
          <PD_VOLUME_CERT_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_CERT_PARAMETER>
          <PD_VOLUME_USER_PASSWORD_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_
             USER_PASSWORD_
             PARAMETER>
          <PD_USER_PASSWORD>PD_RANDOM_VOLUME_PWD</PD_USER_PASSWORD>
         </FUNCTION>
</CSSFile>
```

INITIALIZE_SYSTEM_FUNCTION

このコマンドは、システムで使用する Client Security Solution に対してシステムを初期設定します。システム全体の鍵は、すべてこのファンクション呼び出しにより生成されます。パラメーターは次のとおりです。

- **NEW_OWNER_AUTH_DATA_PARAMETER**

  所有者パスワードはシステムの初期設定を行います。所有者パスワードが設定されていない場合、この引数に対して渡された値は新規所有者パスワードになります。所有者パスフレーズが既に設定され、管理者が同じパスワードを使用する場合は、そのパスワードが渡されます。管理者が新規所有者パスフレーズを使用する場合、希望したパスワードがこのパラメーターへ渡される必要があります。

- **CURRENT_OWNER_AUTH_DATA_PARAMETER**

  システムの現行所有者パスワード。既にシステムに 5.4x 所有者パスワードがある場合は、このパラメーターは 5.4x パスワードをパスする必要があります。それ以外の場合で、新規所有者パスワードを使用する場合は、現行所有者パスワードをこのパラメーターに渡す必要があります。パスワードを変更したくない場合は、値 NO_CURRENT_OWNER_AUTH を渡す必要があります。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>INITIALIZE_SYSTEM_FUNCTION</COMMAND>
          <NEW_OWNER_AUTH_DATA_PARAMETER>pass1word</NEW_OWNER_AUTH_DATA_
              PARAMETER>
          <CURRENT_OWNER_AUTH_DATA_PARAMETER>No_CURRENT_OWNER_AUTH</CURRENT
              _OWNER_AUTH_DATA_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

CHANGE_TPM_OWNER_AUTH_FUNCTION

このコマンドは、Client Security Solution 管理者権限を変更し、それに応じてシステム鍵を更新します。システム全体の鍵は、すべてこのファンクション呼び出しにより再生成されます。パラメーターは次のとおりです。

- NEW_OWNER_AUTH_DATA_PARAMETER

  TPM の新規所有者パスワード

- CURRENT_OWNER_AUTH_DATA_PARAMETER

  TPM の現行所有者パスワード

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>CHANGE_TPM_OWNER_AUTH_FUNCTION</COMMAND>
          <NEW_OWNER_AUTH_DATA_PARAMETER>newPassWord</NEW_OWNER_AUTH_DATA_
              PARAMETER>
          <CURRENT_OWNER_AUTH_DATA_PARAMETER>oldPassWord</CURRENT_OWNER_AUTH
              _DATA_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENROLL_USER_FUNCTION

このコマンドは、Client Security Solution を使用する特定のユーザーを登録します。このファンクションは、ユーザー固有のセキュリティー・キーのすべてを所定のユーザーに作成します。パラメーターは次のとおりです。

- **USER_NAME_PARAMETER**

  登録するユーザーのユーザー名
- **DOMAIN_NAME_PARAMETER**

  登録するユーザーのドメイン名
- **USER_AUTH_DATA_PARAMETER**

  ユーザーのセキュリティー・キーを作成するための TPM パスフレーズ/Windows パスワード
- **WIN_PW_PARAMETER**

  Windows パスワード

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENROLL_USER_FUNCTION</COMMAND>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <USER_AUTH_DATA_PARAMETER>myCssUserPassPhrase</USER_AUTH_DATA_PARAMETER>

          <WIN_PW_PARAMETER>myWindowsPassword</WIN_PW_PARAMETER>
          <VERSION>1.0</VERSION>
          </FUNCTION>
</CSSFile>
```

USER_PW_RECOVERY_FUNCTION

このコマンドは、特定の TPM ユーザーのパスワード・リカバリーをセットアップします。パラメーターは次のとおりです。

- **USER_NAME_PARAMETER**

  登録するユーザーのユーザー名
- **DOMAIN_NAME_PARAMETER**

  登録するユーザーのドメイン名
- **USER_PW_REC_QUESTION_COUNT**

  ユーザーが応答しなければならない質問の数
- **USER_PW_REC_ANSWER_DATA_PARAMETER**

  特定の質問に対する、保管されている応答。このパラメーターの実名には、応答される質問に対応する番号が連結していることに注意してください。次の、このコマンドの例を参照してください。
- **USER_PW_REC_STORED_PASSWORD_PARAMETER**

  質問のすべてが正確に応答されると、ユーザーに示される保管されたパスワード。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>USER_PW_RECOVERY_FUNCTION</COMMAND>
```

```
            <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
            <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
            <USER_PW_REC_ANSWER_DATA_PARAMETER>Test1</USER_PW_REC_ANSWER_DATA_PARA
                METER>
            <USER_PW_REC_ANSWER_DATA_PARAMETER>Test2</USER_PW_REC_ANSWER_DATA_PARA
                METER>
            <USER_PW_REC_ANSWER_DATA_PARAMETER>Test3</USER_PW_REC_ANSWER_DATA_PARA
                METER>
            <USER_PW_REC_QUESTION_COUNT>3</USER_PW_REC_QUESTION_COUNT>
            <USER_PW_REC_QUESTION_LIST>20000,20001,20002</USER_PW_REC_QUESTION_LIST>
           </USER_PW_REC_STORED_PASSWORD_PARAMETER>Pass1word</USER_PW_REC_STORED_PASS
                WORD_PARAMETER>
            <VERSION>1.0</VERSION>
           </FUNCTION>
</CSSFile>
```

SET_WIN_PE_LOGON_MODE_FUNCTION

このコマンドは、 Rescue and Recovery ワークスペース環境に入るときに、ユーザー権限を必要とするかどうかを決めるためにプログラムが読み取るフラグを書き込みます。パラメーターは次のとおりです。

- **WIN_PE_LOGON_MODE_AUTH_PARAMETER**

  次の 2 つの有効な選択項目があります。

  – NO_AUTH_REQUIRED_FOR_WIN_PE_LOGON

  – AUTH_REQUIRED_FOR_WIN_PE_LOGON

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
           <FUNCTION>
            <ORDER>0001</ORDER
            <COMMAND>SET_WIN_PE_LOGON_MODE_FUNCTION</COMMAND>
            <VERSION>1.0</VERSION>
            <WIN_PE_LOGON_MODE_AUTH_PARAMETER>AUTH_REQUIRED_FOR_WIN_PE_LOGON</WIN
                _PE_LOGON_MODE_AUTH_PARAMETER>
            <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
           </FUNCTION>
</CSSFile>
```

第 5 章 System Migration Assistant のカスタマイズ

System Migration Assistant のカスタマイズ可能な部分は、次の 2 つです。

- コマンド・ファイルの編集または変更
- 追加アプリケーション設定の移行

コマンド・ファイルの作成

取り込みフェーズで、SMA はコマンド・ファイルとアーカイブ設定の内容を読み取ります。このセクションでは、コマンド・ファイルおよびその中に指定できるステートメントについて説明します。

System Migration Assistant にはデフォルトのコマンド・ファイル (command.xml) があり、このファイルをテンプレートとして使用して、コマンド・ファイルをカスタマイズすることができます。 SMA をデフォルトの場所にインストールした場合、このファイルは D:¥%RR%¥migration¥bin ディレクトリーにあります。

注: System Migration Assistant 5.0 では、XML テクノロジーを使用して、コマンド・ファイル内のコマンドを記述します。

SMA 5.0 コマンド・ファイルについては、以下の点を考慮に入れてください。

- コマンド・ファイルは XML バージョン 1.0 構文に準拠します。このコマンド・ファイルは、大文字と小文字を区別します。
- 各コマンドおよびパラメーター・セクションは、必ず <TagName> で始まり、</TagName> で終わり、これらのタグの間でその値について記述する必要があります。
- 構文エラーがあると、SMA の実行時にエラーになります。 SMA にエラーが発生すると、 SMA はエラーをログ・ファイルに書き込んで操作を続行します。エラーの重大度により、正しい最終結果が得られない可能性があります。

コマンド・ファイルのコマンド

次の表は、コマンド・ファイルに使用できるコマンドを示したものです (ただし、ファイルの移行とレジストリーに関するコマンドを除きます)。

表 10.

コマンド	パラメーター	パラメーター値と例
<Desktop>	• <accessability> • <active_desktop> • <colors> • <desktop_icons> • <display> • <icon_metrics> • <keyboard> • <mouse> • <pattern> • <screen_saver> • <sento_menu> • <shell> • <sound> • <start_menu> • <taskbar> • <wallpaper> • <window_metrics>	デスクトップ設定を選択するには、このパラメーターを「true」に設定します。それ以外の場合は、「false」に設定するか、指定解除しておきます。 例: `<Desktop>` `<colors>true</colors>` `<desktop_icons>true</desktop_icons>` `<screen_saver>true</screen_saver>` `<start_menu>false</start_menu>` `<time_zone>true</time_zone>` `</Desktop>`
<Network>	• <ip_subnet_gateway_configuration> • <dns_configuration> • <wins_configuration> • <computer_name> • <computer_description> • <domain_workgroup> • <mapped_drives> • <shared_folders_drives> • <dialup_networking> • <odbc_datasources>	デスクトップ設定を選択するには、このパラメーターを「true」に設定します。それ以外の場合は、「false」に設定するか、指定解除しておきます。 例: `<Network>` `<computer_name>true<computer_name>` `<mapped_drives>false</mapped_drives>` `</Network>`
<Applications>	<Application> サポートされているアプリケーションの全リストは、「*ThinkVantage System Migration Assistant* ユーザーズ・ガイド」を参照してください。	例: `<Applications>` `<Application>Lotus Notes</Application>` `<Application>Microsoft Office</Application>` `<//Applications>` または `<Applications>` `<Application>$(all)</Applications>`
<Registries>	• <Registry> • <hive> • <keyname> • <value>	レジストリー設定の取り込みまたは適用を行うには、コマンド・ファイルのパラメーターとして hive、keyname および value を指定します。

表 10. (続き)

コマンド	パラメーター	パラメーター値と例
<IncUsers>	<UserName>	すべてのユーザー・プロファイルを取り込むには、「$(all)」を設定するか、すべてのユーザーを表すワイルドカード文字として「*」を使用します。それ以外の場合は、ユーザーを個別に指定します。 次のワイルドカードが使用可能です。 • * は可変長のワイルドカード用です。 • % は固定長のワイルドカード (1 文字) 用です。 例: <IncUsers> <UserName>administrator</UserName> <UserName>domain¥Jim</UserName> </IncUsers>
<ExcUsers>	<UserName>	移行処理からユーザーを除外するには、ユーザーのドメインおよびユーザー名を指定します。 次のワイルドカードが使用可能です。 • * は可変長のワイルドカード用です。 • % は固定長のワイルドカード (1 文字) 用です。
<Printers>	<Printer> <PrinterName>	この制御ステートメントは、ソース PC とターゲット PC の両方で有効です。 すべてのプリンターを取り込むには、このパラメーターを *&(all)* に設定します。それ以外の場合は、各プリンターを個別に指定します。デフォルト・プリンターのみを取り込む場合は、このパラメーターを *&(DefaultPrinter)* に設定します。 例: <Printers> <Printer>&(all)</Printer> </Printers> <Printers> <Printer> <PrinterName>IBM 5589-L36</PrinterName> </Printer> </Printers> <Printers> <Printer>&(DefaultPrinter)</Printer> </Printers>

表 10. (続き)

コマンド	パラメーター	パラメーター値と例
<MISC>	<bypass_registry>	レジストリー設定の選択をすべて解除するには、「true」に設定します。それ以外の場合は、「false」に設定するか、指定解除しておきます。
	<overwrite existing files>	既存のファイルを上書きするには、「true」に設定します。それ以外の場合は、「false」に設定するか、指定解除しておきます。
	<log_file_location>	SMA でログ・ファイルの書き込み先となるディレクトリーを指定するには、完全修飾ディレクトリー名を入力します。 他のシステムの共用ディレクトリーを指定できます。 このパラメーターを設定しない場合、SMA はログ・ファイルを d:/InstDir/ に書き込みます。ここで、d はハードディスクのドライブ名、 /InstDir/ は SMA のインストール先ディレクトリーです。
	<temp_file_location>	SMA が一時ファイルを書き込むディレクトリーを指定するには、完全修飾ディレクトリー名を入力します。他のシステムの共用ディレクトリーを指定できます。 このパラメーターを設定しない場合、SMA は一時ファイルを d:/InstDir/etc/data に書き込みます。ここで、d はハードディスクのドライブ名、 /InstDir/ は SMA のインストール先ディレクトリーです。
	<resolve_icon_links>	アクティブ・リンクが設定されたアイコンのみをコピーするには、「true」に設定します。それ以外の場合は、「false」に設定するか、指定解除しておきます。

ファイル移行コマンド

SMA はファイル移行コマンドの処理を次の順序で処理します。最初にファイル組み込みコマンドが実行され、次にファイル除外コマンドがその組み込みファイルから実行されます。

SMA は、ソース PC 上のファイルとフォルダーの元の場所に応じて、ファイルを選択および選択解除します。ファイル・リダイレクト・ステートメントはプロファイルに保存され、適用フェーズで解釈されます。

ファイル名とディレクトリー名の処理では、大文字と小文字は区別されません。

次表では、ファイル移行コマンドについて説明します。すべてのファイル移行コマンドはオプションです。

表 11.

コマンド	パラメーター	作業の内容
<FilesAndFolders>	<run>	ファイル移行の取り込みまたは適用を行うには、このパラメーターを「true」に設定します。それ以外の場合は、「false」に設定するか、指定解除しておきます。 例: `<FilesAndFolders>` `<run>true</run>` `</FilesAndFolders>`
<Exclude_drives>	<Drive>	スキャンからドライブを除外するためにドライブ名を指定します。 例: `<ExcludeDrives>` `<Drive>D</Drive>` `<Drive>E</Drive>` `</ExcludeDrive>`

表 11. (続き)

コマンド	パラメーター	作業の内容
<Inclusions>	<IncDescriptions> <Description> <DateCompare> <Operand> <Date> <SizeCompare> <Operand> <Size> <Dest> <Operation> ここで、 • <Description> は完全修飾ファイル名です。ファイル名とフォルダー名の両方にワイルドカード文字を使用できます。 • <DateCompare> は、作成日に基づいてファイルを指定するためのオプション・パラメーターです。 – <Operand> は NEWER または OLDER のいずれかです。 – <Date> は基本となる日付で、mm/dd/yyyy 形式で表します。 • <SizeCompare> は、サイズに基づいてファイルを指定するためのオプション・パラメーターです。 – <Operand> は LARGER または SMALLER のいずれかです。 – <Size> は MB 単位でのファイル・サイズです。 • <Dest> は、ターゲット・システム上の、ファイルが書き込まれる宛先フォルダーの名前を指定するオプション・パラメーターです。 • <Operation> は、ファイル・パスの処理方法を指定するオプション・パラメーターです。以下のいずれかを指定します。 – P は、ファイルのパスを保存し、<Dest> パラメーターで指定された場所から始まるターゲット・システムにファイルを再作成します。 – R は、ファイルのパスを削除し、<Dest> パラメーターで指定された場所にファイルを直接入れます。	指定されたディレクトリーに入っているすべての一致ファイルを検索します。 例: 例 1 `<IncDescription>` `<Description>c:¥MyWorkFolder¥ls</Description>` `</IncDescription>` **注:** フォルダー名を指定するには、記述の最後に .¥. を付加します。 例 2 `<IncDescription>` `<Descriptin>C:¥MyWorkFolder¥*.*</Decsription>` `<DateCompare>` `<Operand>NEWER</Operand>` `<Date>07/31/2005</Date>` `</DateCompare>` `</IncDescription>` 例 3 `<IncDescription>` `<Description>C:¥MyWorkFolder/*.*</Description>` `<SizeCompare>` `<Operand>SMALLER</Operand>` `<Size>200</Size>` `</SizeCompare>` `</IncDescription>` 例 4 `<IncDescription>` `<Description>C:¥MyWorkFolder¥*.*</Description>` `<Dest>D:¥MyNewWorkFolder</Dest>` `<Operation>` `<IncDescription>`

表 11. (続き)

コマンド	パラメーター	作業の内容
<Exclusions>	<ExDescriptions> <Description> <DateCompare> <Operand> <Date> <SizeCompare> <Operand> <Size> ここで、 • <Description> は、完全修飾ファイル名またはフォルダー名です。ファイル名とフォルダー名の両方にワイルドカード文字を含めることができます。 • <DateCompare> は、作成日に基づいてファイルを選択するためのオプション・コマンドです。 – <Operand> は NEWER または OLDER のいずれかです。 – <Date> は基本となる日付で、mm/dd/yyyy 形式で表します。 • <SizeCompare> は、サイズに基づいてファイルを選択するためのオプション・パラメーターです。 – <Operand> は LARGER または SMALLER のいずれかです。 – <Size> は MB 単位でのファイル・サイズです。	指定されたディレクトリーに入っているすべての一致ファイルを選択解除します。 例: 例 1 `<ExDescription>` `<Description>C:¥YourWorkFolder</Description>` `</ExDescription>` 例 2 `<ExDescription>` `<Description>C:¥YourWorkFolder</Description>` `<DateCompare>` `<Operand>OLDER</Operand>` `<Date>07/31/2005</Date>` `</DateCompare>` `</ExDescription>` 例 3 `<ExDescription>` `<Description>C:¥YourWorkFolder</Description>` `<SizeCompare>` `<Operand>LARGER</Operand>` `<Size>200</Size></SizeCompare>` `</ExDescription>`

ファイル移行コマンドの例

このセクションは、ファイル移行コマンドの例を含みます。これらの例は、ファイル選択を絞り込むために、ファイル組み込みコマンドとファイル除外コマンドを結合する方法を示しています。コマンド・ファイルのファイル処理セクションのみを示します。

取り込みフェーズでのファイルの選択

このセクションは、取り込みフェーズでファイル選択のために使用する 3 つのコード例を示します。

例 1

次のコード例では、.doc 拡張子 (Microsoft Word 文書) のすべてのファイルを選択し、それらのファイルを「d:¥My Documents」ディレクトリーに再配置します。次に、d:¥No_Longer_Used ディレクトリーに入っているすべてのファイルを除外します。

```
<IncDescription>
<Description>*:¥*.doc/s</Description>
<Dest>d:¥My Documents</Dest>
<Operation>r</Operation>
<IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>d:¥No_Longer_Used¥</Description>
</ExcDescription>
</Exclusions>
```

例 2

次のコード例では、d ドライブの内容を選択し、 d ドライブのルートにあるすべてのファイルと .tmp 拡張子のすべてのファイルを除外します。

```
<Inclusions>
<IncDescription>
<Description<d:¥*.*/s<¥Description>
</IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>d:¥*.*</Description>
</ExcDescription>
<ExcDescription>
<Description>*:¥*.tmp/s</Description>
</ExcDescription>
</Exclusions>
```

例 3

次のコード例では、c ドライブの内容全体を選択し、 Windows ディレクトリーを指定する %windir% の下にあるすべてのファイルを除外します。

```
<Inclusions>
<IncDescription>C:¥*.*/s</Description>
</Inclusion>
<Exclusions>
<ExcDescription>
<Description>%windir%¥</Description>
</ExcDescription>
</Exclusions>
```

例 4

次のコード例では、現行ログオン・ユーザーのユーザー・プロファイル・パスである %USERPROFILE% フォルダーの内容全体を選択し、 .dat 拡張子で、「Local Settings」サブフォルダーにあるすべてのファイルを除外します。

```
<Inclusions>
<IncDescription>
<Description>%USERPROFILE%¥</Description>
</IncDescription>
</Inclusions>
<Exclusions>
```

追加アプリケーション設定の移行

注: カスタム・アプリケーション・ファイルを作成する場合は、カスタマイズされた設定のストレージ・ロケーションを含め、アプリケーションについて完全な知識を持っている必要があります。デフォルトでは、いくつかのアプリケーションの設定を移行するように SMA が事前構成されています。SMA によってサポートされるアプリケーションのリストについては、「*System Migration Assistant* ユーザーズ・ガイド」を参照してください。また、カスタム・アプリケーション・ファイルを作成して追加アプリケーションの設定を移行することもできます。

このファイルは、application.xml または application.smaapp という名前で、d:¥%RR%¥Migration¥bin¥Apps に配置されている必要あります。ここで、*Apps* はアプリケーションを示し、 d はハードディスクのドライブ名です。同一アプリケーションのカスタム・アプリケーション・ファイルである application.smaapp と application.xml の両方が存在する場合、application.smaapp が優先されます。

新規アプリケーションをサポートするために、既存のアプリケーション・ファイルをコピーして必要な変更を行うこともできます。たとえば、 Microsoft_Access.xml は既存のアプリケーション・ファイルです。

アプリケーション・ファイルについては、以下の点を考慮してください。

- *application*.xml
  - デフォルトでは、System Migration Assistant がインストールされているときは、 application.xml のみが存在します。
  - 「<!-」と「->」で囲まれた <タグ> は、コメントとして扱われます。例:

```
<!--Files_From_Folders>
<!-Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥Whapi¥*.* /s
</Files_From_Folder>
 <Files_From_Folder>%Personal Directory%¥*.pdf</Files_from_Folder>
</Files_From_folders-->
```

  - 各コマンドは別々のセクションで記述する必要があります。
  - 各セクションは、<AppInfo> や <Install_Directories> などのタグで囲まれたコマンドで始まります。 1 つのセクションに 1 つ以上のフィールドを入力できますが、各フィールドは別々の行に分かれている必要があります。
  - アプリケーション・ファイルに構文エラーが含まれている場合、 SMA の操作は続行され、エラーがログ・ファイルに書き込まれます。

72 ページの表 12 は、アプリケーション・ファイルについての情報を示します。

表 12.

セクション	**コマンド**	**値**	**作業の内容**
<Applications>			
	<Family>	テキスト・ストリング。先行スペースは無視されます。テキスト・ストリングを引用符で囲まないでください。	アプリケーションのバージョンに依存しない固有名を指定します。SMA をバッチ・モードで実行する場合は、このストリングをコマンド・ファイルのアプリケーション・セクションで使用します。 例: `<Family>adobe Acrobat Reader</Family>`
	<SMA_Version>	数値。	SMA バージョン番号を指定します。 以下に例を示します。 `<SMA_Version>SMA 5.0</SMA_Version`
	<App>	*ShortName*。ShortName はアプリケーションのバージョン固有のショート・ネームです。	1 つ以上のアプリケーションのバージョン固有のショート・ネームを指定します。 以下に例を示します。 `<APP>Acrobat_Reader_50</APP>`
<Application ShortName=*ShortName*>。ここで、*ShortName* は「Applications」セクションで指定したアプリケーションのショート・ネームです。			
	<Name>	テキスト・ストリング	アプリケーションの名前を指定します。
	<Version>	数値	アプリケーションのバージョンを指定します。
	<Detects> <Detect>	*Root*, *PathAndKey*	レジストリー・キーを指定します。SMA は、指定されたレジストリー・キーを検索してアプリケーションを検出します。 以下に例を示します。 `<Detects>` `<Detect>` `<hive>HKLM</hive>` `<keyname>Software¥Adobe¥Acrobat Reader¥5.0¥</keyname>` `</Detect>` `</Detects>`

表 12. (続き)

セクション	コマンド	値	作業の内容
<Install_Directories> 例: `<Install_Directories>` `<Install_Directory>` `<OS>WinXP</OS>` `<Registry>` `<hive>HKLM</hive>` `<keyname>Software¥Adobe¥Acrobat Reader¥5.0¥InstallPath</keyname>` `<value>(Default)</value>` `</Registry>` `</Install_Directory>` `<Install_Directory>` `<OS>Win2000</OS>` `<Regsitry>` `<hive>HKLM</hive>` `<keyname>Software¥adobe¥Acrobat Reader¥5.0¥InstallPath</keyname>` `<value>(Default)</value>` `</Registry>` `</Install_Directory>` `</Install_Directories>`			
	<OS>	テキスト・ストリング	OS はオペレーティング・システムを示し、以下のいずれかを指定できます。 • WinXP • Win2000 • WinNT • Win98
	<Registry>	*hive* は、HKLM または HKCU のいずれかです。 *keyname* はキー名です。 *value* は、移行するレジストリー値を指定するオプション・コマンドです。	レジストリーに現れるインストール・ディレクトリーを指定します。アプリケーションのインストール・ディレクトリーを示すレジストリーも指定します。
<Files_From_Folders> オプション			

表 12. (続き)

<table>
<tr><th>セクション</th><th>コマンド</th><th>値</th><th>作業の内容</th></tr>
<tr><td></td><td colspan="2">SMAVariable¥Location[|File][/s]

ここで、
• SMAvariable は、カスタマイズ・ファイルの場所を指定する次のいずれかの変数です。
– %Windows Directory% (オペレーティング・システム・ファイルの場所)
– %Install Directory% (Install_Directories セクションで定義されたアプリケーションの場所)
– %Appdata Directory% (ユーザー・プロファイル・ディレクトリーのサブディレクトリーである Application Data ディレクトリー)
– %LocalAppdata Directory% (ユーザー・プロファイル・ディレクトリーのサブディレクトリーである Local Settings フォルダーの Application Data ディレクトリー)
– %Cookies Directory% (ユーザー・プロファイル・ディレクトリーのサブディレクトリーである Cookies ディレクトリー)
– %Favorites Directory% (ユーザー・プロファイル・ディレクトリーのサブディレクトリーである Favorites ディレクトリー)
– %Personal Directory% (ユーザー・プロファイル・ディレクトリーのサブディレクトリー (My Documents) である Personal ディレクトリー。この環境変数は、Windows NT4 では使用できません。)</td><td>移行したいカスタマイズ・ファイルを指定します。

例:
`<Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥Whapi</Files_And_Folders>`

%AppData Directory%¥Adobe¥Acrobat¥Whapi フォルダー内のファイルが SMA で取り込まれます。サブディレクトリー内のファイルは含まれません。

`<Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥Whapi¥ /s</Files_From_Folder>`

%AppData Directory%¥Adobe¥Acrobat¥Whapi フォルダー内のファイルが SMA で取り込まれます。サブディレクトリー内のファイルも含まれます。

`<Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥Whapi¥*.*</Files_From_Folder>`

%AppData Directory%¥Adobe¥Acrobat¥Whapi フォルダー内のファイルが SMA で取り込まれます。サブディレクトリー内のファイルは含まれません。

`<Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥Whapi¥*.* /s</Files_From_Folder>`

%AppData Directory%¥Adobe¥Acrobat¥Whapi フォルダー内のファイルが SMA で取り込まれます。サブディレクトリー内のファイルも含まれます。

`<Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥Whapi</Files_From_Folder>`

「Whapi」の後ろに「¥」がない場合、 SMA では「Whapi」はフォルダーではなくファイルとして扱われます。</td></tr>
</table>

表 12. (続き)

<table>
<tr><th>セクション</th><th>コマンド</th><th>値</th><th>作業の内容</th></tr>
<tr><td></td><td colspan="2">• *Location* は、完全修飾のファイルまたはディレクトリーを指定します。ワイルドカード文字は、ファイル名には使用できますが、パスには使用できません。 ディレクトリーを指定すると、すべてのファイルがコピーされます。
• *[File]* は、オプション・パラメーターで、 Location がディレクトリーを指定し、File がコピー対象のファイルである場合にのみ使用できます。ワイルドカード文字は、ファイル名には使用できますが、パスには使用できません。
• *[¥s]* はオプション・パラメーターです。[/s] を使用すると、サブディレクトリー内のすべてのファイルがコピーされます。
• SMA5.0 ユーザーは、 Windows 環境変数を使用できます。 SMA を開始したユーザーの環境変数は、 Windows 環境変数の値として使用されます。</td><td></td></tr>
<tr><td colspan="4"><Registries>

オプション</td></tr>
<tr><td></td><td colspan="2">*hive* は、HKLM または HKCU のいずれかです。

keyname はキー名です。 value は、移行するレジストリー値を指定するオプション・コマンドです。</td><td>移行したいレジストリーを指定します。

例:

<Registries>
<Registry>
<hive>HKCU</hive>
<keyname>Software¥Adobe¥Acrobat</keyname>
<value></value>
</Registry>
</Registries></td></tr>
<tr><td colspan="4"><Registry_Excludes>

オプション</td></tr>
</table>

表 12. (続き)

セクション	コマンド	値	作業の内容
	hive は、HKLM または HKCU のいずれかです。 *keyname* はキー名です。 value は、移行するレジストリー値を指定するオプション・コマンドです。		選択したレジストリーから除外したいレジストリー・キーと値を指定します。 例: `<Registry_Excludes>` `<Registry>` `<hive>HKCU</hive>` `<keyname>Software¥Adobe¥Acrobat Reader¥5.0¥AdobeViewer` `</keyname>` `<value>xRes</value>` `</Registry>` `</Registry_Excludes>`
<Files_Through_Registry>			
	<OS> は、オペレーティング・システムを指定し、以下のいずれかの値です。 • WinXP • Win2000 • WinNT • Win98 <Registry> は、レジストリー項目を指定し、 hive、keyname、value のフォーマットになっています。ここで、 • hive は、HKLM または HKCU のいずれかです。 • keyname はキー名です。 • value は、移行するレジストリー値を指定するオプション・コマンドです。 File はファイル名です。ワイルドカード文字を使用できます。 File はファイル名です。ワイルドカード文字を使用できます。		移行するカスタマイズ・ファイルを指定します。 例: `<Files_Through_Registries>` `<Files_Through_Registry>` `<OS>WinXP</OS>` `<Registry>` `<hive>HKCU</hive>` `<keyname>Software¥Lotus¥Organizer¥99.0¥Paths</keyname>` `<value>Backup</value>` `</Registry>` `<File>*.*/s</File>` `</Files_Through_Registry>` `</Files_Through_Registries>`
<PreTargetBatchProcessing>			
	`<PreTargetBatchProcessing>` `<!CDAT[batch commands]]` `<PreTargetBatchProcessing>`		<PreTargetBatchProcessing> は、適用フェーズで <Registries> が処理される前にバッチ処理を実行します。 例: `<PreTargetBatchProcessing>` `<!CDATA[copy /y c:¥temp¥*.* c:¥migration` `del c:¥migration¥*.mp3` `</PreTargetBatchProcessing>`
<TargetBatchProcessing>			

表 12. (続き)

セクション	コマンド	値	作業の内容
	<TargetBatchProcessing> <!CDAT[batch commands]] <TargetBatchProcessing>		<TargetBatchProcessing> は、適用フェーズで <Registries> が処理された後にバッチ処理を実行します。 例: <TargetBatchProcessing> <!CDATA[copy /y c:¥temp¥*.* c:¥migration del c:¥migration¥*.mp3 <TargetBatchProcessing>

アプリケーション・ファイルの作成

カスタム・アプリケーション・ファイル用にどのアプリケーション設定を移行する必要があるかを決定するには、アプリケーションを慎重にテストしなければなりません。

アプリケーション・ファイルを作成するには、以下のステップを完了します。

1. ASCII テキスト・エディターを使用して既存の application.XML ファイルを開きます。 SMA をデフォルトの場所にインストールした場合、 application.XML ファイルは、 d:¥d:¥%RR%¥Migration¥bin¥Apps ディレクトリーに入れられます。ここで、d はハードディスクのドライブ名です。
2. 移行したいアプリケーションとアプリケーション設定についてこの application.XML ファイルを変更します。
3. <Applications> セクションの情報を変更します。
4. <Application Shortname=*Shortname*> セクションの <Name> コマンドと <Version> コマンドを変更します。
5. 移行する必要があるレジストリー・キーを決定します。
   a. 「**スタート**」→「**ファイルを指定して実行**」とクリックします。「ファイルを指定して実行」ウィンドウが開きます。「**名前 (O)**」フィールドに regedit と入力して、「**OK**」をクリックします。「レジストリ エディタ」ウィンドウが開きます。
   b. 左側のペインで「**HKEY_LOCAL_MACHINE**」ノードを展開します。
   c. 「**ソフトウェア (Software)**」ノードを展開します。
   d. ベンダー固有のノード (たとえば、「**Adobe**」) を展開します。
   e. アプリケーションのレジストリー・キーが見つかるまで、調査を続行します。この例では、レジストリー・キーは SOFTWARE¥Adobe¥Acrobat Reader¥6.0 です。
   f. 「Detect」フィールドの値を設定します。例:

```
<Detects>
<Detect
<hive>HKLM</hive>
<keyname>Software¥Adobe|acrobat Reader¥6.0<keyname>
</Detect
</Detects
```

6. Install_Directories セクションの Name コマンドと Version コマンドを変更します。

7. アプリケーションのインストール・ディレクトリーへのパスを確認します。
   a. 「レジストリ エディタ」ウィンドウから、HKLM¥SOFTWARE¥Adobe¥Acrobat Reader¥6.0¥InstallPath ノードにナビゲートします。
   b. 該当するコマンドをアプリケーション・ファイルの Install_Directories セクションに追加します。例:

```
<Install_Directory>
<OS>WinXP</OS>
<Registry>
<hive>HKLM</hive
<keyname>Software¥Adobe¥Acrobat Reader¥6.0¥InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>
```

   注: アプリケーション固有のディレクトリーが HKLM¥Software¥Microsoft¥Windows¥CurrentVersion¥AppPaths ディレクトリーにない場合は、HKLM¥Software ツリー内の他の場所で、インストール・パスを含むディレクトリーを見つける必要があります。ディレクトリーを見つけたら、そのキーを <Install_Directories> セクションで使用します。
8. <Files_From Folders> セクションで、移行したいカスタマイズ・ファイルを指定します。
   a. 多くのアプリケーションは、デフォルトで、ファイルを Documents and Settings サブディレクトリーに保存しているので、Application Data ディレクトリーでこのアプリケーションに関連するディレクトリーを調べてください。 それが存在している場合は、次のコマンドを使用してそのディレクトリーとファイルを移行することができます。

```
<Files_From_Folder>SMAvariable¥Location¥[File] [/s] </Files_From_Folder>
```

   ここで、Location¥ は完全修飾ファイルまたはディレクトリー、 [File] は、Location¥ がディレクトリーを指定する場合に限り使用可能なオプション・パラメーターです。 Adobe Reader の例では、カスタマイズ・ファイルは Preferences ディレクトリーに入っています。
   b. 個人用設定が保存されている可能性があるすべての関連ディレクトリーを調べます。
   c. Local Settings ディレクトリーを調べます。
9. 移行したいレジストリー項目を決定します。それらは HKCU (HKEY_CURRENT_USER) に入っています。アプリケーション・ファイルの <Registries> セクションで、該当するコマンドを追加します。
10. application.XML ファイルを d:¥Program Files¥ThinkVantage¥SMA¥Apps ディレクトリーに保存します。ここで、d はハードディスクのドライブ名です。
11. 新規のアプリケーション・ファイルをテストします。

Adobe Reader 用の application.XML ファイルの例

このセクションでは、Adobe Reader のアプリケーション・ファイルを紹介します。

```
<?xml version="1.0"?>
<Applications>
<Family>Adobe Acrobat Reader</Family>
<SMA_Version>SMA 5.0</SMA_Version>
```

```
<APP>Acrobat_Reader_70</APP>
<APP>Acrobat_Reader_60</APP>
<APP>Acrobat_Reader_50</APP>

<Application ShortName="Acrobat_Reader_50">
<AppInfor>
         <Name>Acrobat_Reader_50</Name>
         <Version>5.0</Version>
         <Detects>
                 <Detect>
                     <hive>HKLM</hive>
                     <keyname>Software¥Adobe¥Acrobat Reader¥5.0</keyanme>
                 </Detect>
         </Detects>
</AppInfo>
<Install_Directories>
            <Install_Directory>
               <OS>WinXP</OS>
               <Registry>
                       <hive>HKLM</hive>
                       <keyname>Software¥Adobe¥Acrobat Reader¥5.0¥InstallPath
</keyname>
                       <value>(Default)</value>
               </Registry>
            </Install_Directory>
            <Install_Direcotry>
               <OS>Win2000</OS>
               <Registry>
                       <hive>HKLM</hive>
                       <keyname>Software¥Adobe¥Acrobat Reader¥5.0¥InstallPath
</keyname>
                       <value>(Default)</value>
               </Registry>
            </Install_Directory>
            <Install_Directory>
                 <OS>Win98</OS>
                 <Registry>
                       <hive>HKLM</hive>
                       <keyname>Software¥Adobe¥Acrobat Reader¥5.0¥InstallPath
<keyname>
                       <value>(Default)</value>
                 </Registry>
            </Install_Directory>
            <Install_Directory>
                 <OS>WinNT</OS>
                 <Registry>
                       <hive>HKLM</hive>
                       <keyname>Software¥Adobe¥Acrobat Reader¥5.0¥InstallPath
</keyname>
                       <value>(Default)</value>
                 </Registry>
            </Install_Directory>
</Install_Directories>

<Files_From_Folders>
           <Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥Whapi¥*.*
/s</Files_From_Folder>
           <Files_From_Folder>%Personal Directory%¥*.pdf</Files_From_Folder>
<Files_From_Folders>
<Files_Through_Registries>
</Files_Through_Registries>

<Registries>
            <Registry>
                       <hive>HKCU</hive>
                       <keyname>Software¥Adobe¥Acrobat</keyname>
             </Registry>
```

```
             <Registry>
                       <hive>HKCU</hive>
                       <keyname>Software¥Adobe¥Acrobat Reader</keyname>
             </Registry>
             <Registry>
                       <hive>HKCU</hive>
                       <keyname>Software¥Adobe¥Persistent Data</keyname>
             </Registry>
</Registries>

<Registry_Excludes>
            <Registry>
                       <hive>HKCU</hive>
                       <keyname>Software¥Adobe¥Acrobat Reader¥5.0¥AdobeViewer
</keyname>
                       <value>xRes</value>
            </Registry>
            <Registry>
                       <hive>HKCU</hive>
                       <keyname>Software¥Adobe¥Acrobat Reader¥5.0¥Adobe¥Viewer
</keyname>
                       <value>yRes</value>
            </Registry>
<Registry_Excludes>

<SourceBatchProcessing>
</SourceBatchProcessing>

<PreTargetBatchProcessing>
</PreTargetBatchProcessing>

<TargetBatchProcessing>
</TargetBatchProcessing>
</Application>
<Application ShortName="Acrobat_Reader_6.0">
        <AppInfo>
                    <Name>Adobe Acrobat Readr 6.0<¥Name>
                           <Version>6.0</Version>
                           <Detects>
                                 <Detect>
                                        <hive>HKLM</hive>
                                        <keyname>Software¥Adobe¥Acrobat Reader¥6.0
</keyname>
                                 </Detect>
                           </Detects>
        <¥AppInfo>
<Install_Directories>
          <Install_Directory>
               <OS>WinXP</OS>
               <Registry>
                         <hive>HKLM</hive>
                         <keyname>Software¥Adobe¥Acrobat Reader¥6.0¥InstallPath
</keyname>
                         <value>(Default)</value>
               </Registry>
          </Install_Directory>
          <Install_Directory>
               <OS>Win2000</OS>
               <Registry>
                         <hive>HKLM</hive>
                         <keyname>Software¥Adobe¥Acrobat Reader¥6.0¥InstallPath
</keyname>
                         <value>(Default)</value>
               </Registry>
          </Install_Directory>
          <Install_Directory>
              <OS>Win98</OS>
```

```
             <Registry>
                       <hive>HKLM</hive>
                       <keyname>Software¥Adobe¥Acrobat Reader¥6.0¥InstallPath
</keyname>
                       <value>(Default)</value>
            </Registry>
        </Install_Directory><Install_Directory>
            <OS>WinNT</OS>
            <Registry>
                      <hive>HKLM</hive>
                      <keyname>Software¥Adobe¥Acrobat Reader¥6.0¥InstallPath
</keyname>
                      <value>(Default)</value>
            </Registry>
        </Install_Directory>
</Install_Directories>

<Files_From_Folders>
           <Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥6.0¥*.* /s
</Files_From_Folder>
           <Files_From_Folder>%Personal Directory%¥*.pdf</Files_From_Folder>
</Files_From_Folders>

<Files_Trough_Registries>
</Files_Trough_Registries>

<Registries>
            <Registry>
                      <hive>HKCU</hive>
                      <keyname>Software¥Adobe¥Acrobat</keyname>
            </Registry>
            <Registry>
                      <hive>HKCU</hive>
                      <keyname>Software¥Adobe¥Acrobat Reader</keyname>
            </Registry>
</Registries>

<Registry_Excludes>
            <Registry>
                      <hive>HKCU</hive>
                      <keyname>Software¥Adobe¥Acrobat Reader¥6.0¥AdobeViewer
</keyname>
                      <value>xRes</value>
            </Registry>
            <Registry>
                      <hive>HKCU</hive>
                      <keyname>Software¥Adobe¥Acrobat Reader¥6.0¥Adobe¥Viewer
</keyname>
                      <value>yRes</value>
            </Registry>
<Registry_Excludes>

<SourceBatchProcessing>
</SourceBatchProcessing>

<PreTargetBatchProcessing>
</PreTargetBatchhProcessing>

<TargetBatchProcessing>
           <![CDATA[
          if /i "%SourceApp%" == "Acrobat_Reader_50" goto Update50
          goto Done
          :Update50
          regfix "HKCU¥Software¥Adobe¥Acrobat Reader¥5.0" "HKCU¥Software¥Adobe¥
Acrobat Reader¥6.0"
          regfix "HKLM¥Software¥Adobe¥Acrobat Reader¥5.0¥AdobeViewer" "HKLM¥
Software¥Adobe¥Acrobat Reader¥6.0¥AdobeViewer"
```

```
          :Done
]]>
</TargetBatchProcessing>
</Application>

<Application ShortName="Acrobat_Reader_7.0">
              <AppInfo>
                        <Name>Adobe Acrobat Reader 7.0<¥Name>
                        <Version>6.0</Version>
                        <Detects>
                                 <Detect>
                                 <hive>HKLM</hive>
                                 <keyname>Software¥Adobe¥Acrobat Reader
¥7.0</keyname>
                                 </Detect>
                        </Detects>
             <¥AppInfo>
<Install_Directories>
              <Install_Directory>
                           <OS>WinXP</OS>
                           <Registry>
                                 <hive>HKLM</hive>
                                 <keyname>Software¥Adobe¥Acrobat Reader¥7.0¥
InstallPath</keyname>
                                 <value>(Default)</value>
                           </Registry>
              </Install_Directory>
              <Install_Directory>
                           <OS>Win2000</OS>
                           <Registry>
                                     <hive>HKLM</hive>
                                     <keyname>Software¥Adobe¥Acrobat Reader¥7.0¥
InstallPath</keyname>
                                     <value>(Default)</value>
                           </Registry>
              </Install_Directory>
<Install_Directory>
                           <OS>Win98</OS>
                           <Registry>
                                     <hive>HKLM</hive>
                                     <keyname>Software¥Adobe¥Acrobat Reader¥7.0¥
InstallPath</keyname>
                                     <value>(Default)</value>
                           </Registry>
              </Install_Directory><Install_Directory>
                           <OS>WinNT</OS>
                           <Registry>
                                     <hive>HKLM</hive>
                                     <keyname>Software¥Adobe¥Acrobat Reader¥7.0¥
InstallPath</keyname>
                                     <value>(Default)</value>
                            </Registry>
              </Install_Directory>
</Install_Directories>

<Files_From_Folders>
            <Files_From_Folder>%AppData Directory%¥Adobe¥Acrobat¥7.0¥*.* /s
</Files_From_Folder>
            <Files_From_Folder>%Personal Directory%¥*.pdf</Files_From_Folder>
</Files_From_Folders>

<Files_Trough_Registries>
</Files_Trough_Registries>

<Registries>
            <Registry>
                      <hive>HKCU</hive>
```

```
                    <keyname>Software¥Adobe¥Acrobat</keyname>
            </Registry>
            <Registry>
                    <hive>HKCU</hive>
                    <keyname>Software¥Adobe¥Acrobat Reader</keyname>
            </Registry>
</Registries>

<Registry_Excludes>
            <Registry>
                    <hive>HKCU</hive>
                    <keyname>Software¥Adobe¥Acrobat Reader¥7.0¥AdobeViewer
</keyname>
                    <value>xRes</value>
           </Registry>
           <Registry>
                    <hive>HKCU</hive>
                    <keyname>Software¥Adobe¥Acrobat Reader¥7.0¥Adobe¥Viewer
</keyname>
                    <value>yRes</value>
           </Registry>
<Registry_Excludes>

<SourceBatchProcessing>
</SourceBatchProcessing>

<PreTargetBatchProcessing>
</PreTargetBatchProcessing>

TargetBatchProcessing>
           <![CDATA[
          if /i "%SourceApp%" == "Acrobat_Reader_50" goto Update50
          if /i "%SourceApp%" == "Acrobat_Reader_60" goto Update60
          goto Done
          :Update50
          regfix "HKCU¥Software¥Adobe¥Acrobat Reader¥5.0" "HKCU¥Sof
tware¥Adobe¥Acrobat Reader¥7.0"
          regfix "HKLM¥Software¥Adobe¥Acrobat Reader¥5.0¥AdobeView
er" "HKLM¥Software¥Adobe¥Acrobat Reader¥7.0¥AdobeViewer"
          goto Done
          :Update60
regfix "HKCU¥Software¥Adobe¥Acrobat Reader¥6.0" "HKCU¥Softw
are¥Adobe¥Acrobat Reader¥7.0"
          regfix "HKLM¥Software¥Adobe¥Acrobat Reader¥6.0¥AdobeVi
ewer" "HKLM¥Software¥Adobe¥Acrobat Reader¥7.0¥AdobeViewer"
          :Done
          ]]>
</TargetBatchProcessing>
</Application>

</Applications>
```

システム更新

Active Update

Active Update Launcher がインストール済みかどうかを判別するには、次のレジストリー・キーの存在を確認します。

```
HKLM¥Software¥TVT¥ActiveUpdate
```

Active Update Launcher が Active Update を許可するように構成されているかどうかを判別するために、 TVT は自分のレジストリー・キー内を調べ、

EnableActiveUpdate 属性の値の有無を確かめます。If EnableActiveUpdate=1 の場合は、 TVT はヘルプ・メニューの下に ActiveUpdate メニュー項目を追加します。

Active Update を呼び出すために TVT を呼び出すと、 Active Update Launcher プログラムが起動し、パラメーター・ファイルが渡されます。

Active Update を起動するには、次の手順に従います。

1. 次の Active Update Launcher レジストリー・キーを開く。

   ```
   HKLM¥software¥TVT¥ActiveUpdate
   ```
2. Path 属性の値を取得する。
3. Program 属性の値を取得する。

第 6 章 インストール

Rescue and Recovery/Client Security Solution のインストール・パッケージは、InstallShield 10.5 Premier によって Basic MSI プロジェクトとして開発されました。 InstallShield 10.5 Basic MSI プロジェクトは、 Windows インストーラを使用して、アプリケーションをインストールします。これにより、管理者には、コマンド・ラインからのプロパティ値の設定などの、インストールをカスタマイズする多くの機能が提供されます。以下のセクションでは、 Rescue and Recovery 3.0 セットアップ・パッケージを使用および実行方法について説明します。より正しく理解するために、パッケージのインストールを開始する前に、まず章全体をお読みください。

注: このパッケージをインストールするときは、以下の Lenovo Web ページに掲載されている README ファイルを参照してください。

http://www.lenovo.com/ThinkVantage (英語のサイトです。)
http://www.ibm.com/jp/pc/think/thinkvantagetech.shtml (日本語のサイトです。)

README ファイルには、ソフトウェア・バージョン、サポートされるシステム、システム要件、およびインストール・プロセスに役立つその他の考慮事項などのテーマに関する最新の情報が含まれています。

インストール要件

このセクションでは、 Rescue and Recovery/Client Security Solution パッケージをインストールするためのシステム要件を説明します。最良の結果を得るために、次の Web サイトにアクセスして、ソフトウェアが最新版であることを確認してください。

http://www.lenovo.com/ThinkVantage (英語のサイトです。)
http://www.ibm.com/jp/pc/think/thinkvantagetech.shtml (日本語のサイトです。)

IBM から以前に販売された PC でも、指定された要件を満たしていれば、Rescue and Recovery がサポートされます。Rescue and Recovery がサポートされる IBM PC について詳しくは、 Web のダウンロード・ページを参照してください。

IBM および Lenovo PC の要件

IBM および Lenovo PC が Rescue and Recovery を実行するには、次の要件を満たしているか、それ以上であることが必要です。

- オペレーティング・システム: Microsoft Windows XP SP1 または Windows 2000 SP3 以上
- プロセッサー: Microsoft により Windows XP (Home または Professional) および Windows 2000 のインストール要件として指定されているもの
- メモリー: 256 MB 以上推奨
  - 共用メモリー設定の場合、共用メモリーの BIOS 設定を 4 MB から 8 MB までの間に設定する必要があります。

– 非共用メモリー設定の場合、非共用メモリーは 120 MB 以上です。

注: PC の非共用メモリーが 200 MB 未満である場合でも、 Rescue and Recovery は稼働します。ただし、Rescue and Recovery ワークスペースで複数のアプリケーションを起動することができない場合があります。

- ハードディスク空き容量 2.4 GB 以上 (プログラムのインストールには 2.8 GB が必要であり、これには Rescue and Recovery のバックアップに必要なスペースは含まれません)
- 解像度 800 x 600 および 24 ビット・カラーをサポートする VGA 対応ビデオ
- サポートされるイーサネット・カード

Rescue and Recovery のインストール・コンポーネント

1. 主なインストール・パッケージ (約 45 MB): これは、インストール・プロジェクト・ソースからビルドされた setup.exe です。 setup.exe ファイルは、ビルド・プロセス中に、プロジェクト ID、メディア・タイプ、ビルド・レベル、国別コード (この場合は、常に US)、およびパッチ・コードを表す名前 (たとえば、 Z096ZIS1001US00.exe) に変更されます。これは、インストール・ソース・ファイルを解凍し、 Windows インストーラを使用してインストールを起動する自己解凍型インストール・パッケージです。このファイルには、インストール・ロジックと Windows アプリケーション・ファイルが含まれています。パッケージには、ワークスペース・ファイルは含まれていません。
2. Predesktop US Base (約 135 MB): これは、パスワードで保護された ZIP ファイルで、 US ベースのワークスペース全体が含まれています。その名前の形式は、Z062ZAA1001US00.TVT です。この場合、*AA* は、ワークスペースの互換性を決定し、 *001* はワークスペースのレベルです。このファイルは、すべての言語システムにワークスペースをインストールする際に必要です。このファイルは、メイン・インストール・パッケージ (解凍または OEM インストールの場合は、setup.exe または Rescue and Recovery/Client Security Solution.msi のいずれか) と同じディレクトリーになければなりません。この場合の例外は、ワークスペースがすでにインストール済みでアップグレードする必要がない場合、またはインストールを実行する際にコマンド・ラインでプロパティ PDA=0 が設定されており、ワークスペース (あらゆるバージョン) がまだ存在していない場合です。setup.exe には、ファイル pdaversion.txt が含まれています。このファイルには、Windows のそのバージョンと連動可能なワークスペースの最小バージョンが含まれています。 setup.exe インストーラは、次のロジックを使用してワークスペースを探します。
   - **古い Predesktop (RNR 1.0 または 2.X) が存在するか、 Predesktop が存在しない場合:**

     インストーラは、最小バージョンの互換コードと等しい互換コード (たとえば、AA、AB) を持ち、レベルが最小バージョン (.TVT ファイル名のその他のバージョン・フィールドは、すべて最小バージョンに完全に一致しなければなりません) 以上の .TVT を探します。これらの基準を満たすファイルが見つからない場合、インストールは停止します。
   - **新しい (RNR 3.0) Predesktop が存在する場合:**

インストーラは、現在のワークスペースの互換コードを最小バージョンの互換コードと比較し、その結果に基づいて以下の処理を行います。

– **現在の®コードが最小コードより大きい場合:**

  インストーラは、現在の環境はこのバージョンの RNR と互換性がないというメッセージを表示します。

– **現在のコードと最小コードが同じである場合:**

  インストーラは、現行バージョンのレベルを最小バージョンのレベルと比較します。現行バージョンのレベルが最小バージョンのレベル以上である場合、インストーラは、最小バージョンの互換コードと等しい互換コード (AA、AB...) を持ち、そのレベルが現行バージョンのレベルより高い .TVT ファイル (.TVT ファイル名のその他のバージョン・フィールドは、すべて最小バージョンに完全に一致しなければなりません) を探します。インストーラがファイルを見つけられない場合、インストール・プロセスはワークスペースを更新せずに続行されます。現在のレベルが最低レベル未満である場合、インストーラは、最小バージョンの互換コードと等しい互換コード (AA、AB、...) を持ち、レベルが最小バージョンのレベル以上の .TVT ファイル (.TVT ファイル名のその他のバージョン・フィールドは、すべて最小バージョンに完全に一致しなければなりません) を探します。これらの基準を満たすファイルが見つからない場合、インストールは停止します。

– **現在のコードが最小コードより小さい場合:**

  インストーラは、最小バージョンの互換コードと等しい互換コード (AA、AB、...) を持ち、レベルが最小バージョン (.TVT ファイル名のその他のバージョン・フィールドは、すべて最小バージョンに完全に一致しなければなりません) 以上の .TVT を探します。これらの基準を満たすファイルが見つからない場合、インストールは停止します。

3. Predesktop の言語パック (それぞれ約 5 から 30 MB): Rescue and Recovery 3.0 でサポートされる Rescue and Recovery ワークスペースの場合は、 24 の言語パックがあります。各言語パックは、Z062ZAA1001CC00.TVT 形式で命名されており、この場合、CC は言語を表します。英語以外のシステム、またはサポートされない言語のシステムにワークスペースをインストールする場合は、これらのファイルのいずれかが必要です。また、そのファイルは、メイン・インストールおよび US ワークスペースの .TVT ファイルと同じディレクトリーに置く必要があります。 Windows が英語以外である場合、または言語がその言語パックでサポートされていない場合は、言語パックの言語が Windows の言語と一致しなければなりません。ワークスペースをインストールまたは更新する際に言語パックが必要になると、インストールは .TVT 言語パックを探します。この場合、ファイル名のすべてのフィールドは、言語コード (システムの言語と一致しなければならない) を除き、 US ワークスペースのファイル名と一致しなければなりません。言語パックは、以下の言語で使用可能です。
   - アラビア語
   - ブラジル・ポルトガル語
   - ポルトガル語
   - チェコ語
   - デンマーク語

- フィンランド語
- フランス語
- ギリシャ語
- ドイツ語
- ヘブライ語
- 香港語
- ハンガリー語
- イタリア語
- 日本語
- 韓国語
- オランダ語
- ノルウェー語
- ポーランド語
- ポルトガル語
- ロシア語
- 中国語 (簡体字)
- スペイン語
- スウェーデン語
- 中国語 (繁体字)
- トルコ語

標準的なインストール手順およびコマンド・ライン・パラメーター

setup.exe は、以下に説明する一連のコマンド・ライン・パラメーターを受け入れます。コマンド・ライン・オプションには、パラメーターを指定することが必要です。この場合、オプションとパラメーターの間にスペースは入れません。たとえば、Setup.exe /s /v″/qn REBOOT=”R”″ は有効ですが、 Setup.exe /s /v ″/qn REBOOT=”R”″ は無効です。オプションのパラメーターは、そのパラメーターにスペースが含まれている場合に限り、引用符で囲む必要があります。

注: インストールを単独で実行すると (パラメーターを指定せずに setup.exe だけを実行すると)、デフォルトでは、インストール終了時にユーザーに再起動を促すプロンプトが出されます。プログラムを正しく機能させるには、再起動する必要があります。上記および例のセクションで示すように、サイレント・インストールではコマンド・ライン・パラメーターを使用して再起動を遅らせることができます。

以下のパラメーターと説明は、InstallShield Developer のヘルプ文書化から直接引用したものです。基本 MSI プロジェクトに適用されないパラメーターは、除かれています。

表 13.

パラメーター	説明
/a : 管理用インストール	/a スイッチを指定すると、Setup.exe で管理用インストールが実行されます。管理用インストールは、データ・ファイルをユーザーが指定したディレクトリーにコピー (および解凍) しますが、ショートカットの作成、COM サーバーの登録、アンインストール・ログの作成は行いません。
/x : アンインストール・モード	/x スイッチを指定すると、Setup.exe は以前にインストールした製品をアンインストールします。
/s : サイレント・モード	コマンド Setup.exe /s を実行すると、基本 MSI インストール・プログラム用の Setup.exe 初期設定ウィンドウは表示されず、応答ファイルは読み取られません。基本 MSI プロジェクトでは、サイレント・インストールの場合、応答ファイルは作成も使用もされません。基本 MSI 製品をサイレントで実行するには、コマンド・ライン Setup.exe /s /v/qn を実行します。 (基本 MSI のサイレント・インストールの共通プロパティ値を指定する場合は、 Setup.exe /s /v″/qn INSTALLDIR=D:¥Destination″ などのコマンドを使用できます。)
/v : Msiexec への引数の受け渡し	/v 引数を使用して、 Msiexec.exe にコマンド・ライン・スイッチと共通プロパティの値を渡します。
/L : 言語のセットアップ	ユーザーは、/L スイッチと 10 進言語 ID を使用して、複数言語インストール・プログラムで使用する言語を指定します。たとえば、ドイツ語を指定するコマンドは Setup.exe /L1031 です。注: 表 14 に記載されているすべての言語のインストールがサポートされているわけではありません。
/w : 待機	基本 MSI プロジェクトで引数 /w を指定すると、Setup.exe は、インストールが完了するのを待ってから終了します。バッチ・ファイルで /w オプションを使用すると、Setup.exe のコマンド・ライン引数全体を start /WAIT で開始することができます。正しくフォーマットされたコマンドの使用例は、次のとおりです。 `start /WAIT setup.exe /w`

表 14.

言語	ID
アラビア語 (サウジアラビア)	1025

表 14. (続き)

言語	**ID**
バスク語	1069
ブルガリア語	1026
カタロニア語	1027
中国語 (簡体字)	2052
中国語 (繁体字)	1028
クロアチア語	1050
チェコ語	1029
デンマーク語	1030
オランダ語 (標準)	1043
英語	1033
フィンランド語	1035
カナダ・フランス語	3084
フランス語	1036
ドイツ語	1031
ギリシャ語	1032
ヘブライ語	1037
ハンガリー語	1038
インドネシア語	1057
イタリア語	1040
日本語	1041
韓国語	1042
ノルウェー語 (ブークモール)	1044
ポーランド語	1045
ポルトガル語 (ブラジル)	1046
ポルトガル語 (標準)	2070
ルーマニア語	1048
ロシア語	1049
スロバキア語	1051
スロベニア語	1060
スペイン語	1034
スウェーデン語	1053
タイ語	1054
トルコ語	1055

管理用インストールの手順およびコマンド・ライン・パラメーター

Windows インストーラは、ワークグループによる使用またはカスタマイズのために、アプリケーションまたは製品のネットワークへの管理用インストールを実行できます。Rescue and Recovery/Client Security Solution インストール・パッケージの場合、管理用インストールによりインストール・ソース・ファイルが指定された場

所に解凍されます。管理用インストールを実行するには、セットアップ・パッケージをコマンド・ラインから /a パラメーターを使用して実行する必要があります。

```
Setup.exe /a
```

管理用インストールを実行すると、管理者にセットアップ・ファイルの解凍先を指定するようプロンプトを出す一連のダイアログ画面が表示されます。管理者に示されるデフォルトの解凍先は C:¥ です。新しい解凍先は、C: 以外のドライブ (他のローカル・ドライブおよび接続されたネットワーク・ドライブなど) を含む場所から選択できます。新しいディレクトリーも、この手順で作成できます。

管理用インストールをサイレント・インストールで実行する場合、解凍先の場所を指定するために、コマンド・ラインで次のように共通プロパティ TARGETDIR を設定することができます。

```
Setup.exe /s /v"/qn TARGETDIR=F:¥TVTRR"
```

管理用インストールが完了した後、管理者はソース・ファイルをカスタマイズ (たとえば、設定値を tvt.txt に追加) することができます。カスタマイズした後に解凍したソースからインストールするには、ユーザーはコマンド・ラインで msiexec.exe を実行し、解凍された msi ファイルの名前を引き渡します。

次のセクションでは、msiexec で有効なコマンド・ライン・パラメーターと、その使用方法を説明します。共通プロパティは、msiexec コマンド・ライン呼び出しで直接設定することもできます。

MsiExec.exe コマンド・ライン・パラメーター

MsiExec.exe は、Windows インストーラの実行可能プログラムで、インストール・パッケージを解釈し、製品をターゲット・システムにインストールするために使用されます。

```
msiexec. /i "C:WindowsFolder/Profiles¥UserName¥Persona¥MySetups¥project name¥
product configuration¥release name¥DiskImages¥Disk1¥product name.msi
```

次の表に、MsiExec.exe コマンド・ライン・パラメーターの詳細な説明を示します。この表は、Windows インストーラに関する Microsoft Platform SDK 文書からの引用です。

表 15.

パラメーター	説明
/i *package* または *product code*	たとえば、Othello という名称の製品をインストールする場合、以下のように行います。 `msiexec /i "C:¥WindowsFolder¥Profiles¥UserName¥Personal¥MySetups¥Othello¥Trial Version¥Release¥DiskImages¥Disk1¥Othello Beta.msi"` 製品コードとは、製品のプロジェクト・ビューの製品コード・プロパティで自動的に生成される GUID のことです。

表 15. (続き)

パラメーター	説明
/f [p|o|e|d|c|a|u|m|s|v] *package* または *product code*	インストール時に /f オプションを指定すると、欠落または破損したファイルが修復または再インストールされます。 たとえば、すべてのファイルを強制的に再インストールするには、次の構文を使用します。 `msiexec /fa "C:¥WindowsFolder¥Profiles¥UserName¥Personal¥MySetups¥Othello¥Trial Version¥Release¥DiskImages¥Disk1¥Othello Beta.msi"` 以下のフラグを結合することができます。 • p は、欠落したファイルを再インストールします。 • o は、ファイルが欠落している場合、またはユーザーのシステムに存在するファイルのバージョンが古い場合に、そのファイルを再インストールします。 • e は、ファイルが欠落している場合、またはユーザーのシステム上に同等のファイルまたは旧バージョンのファイルが存在する場合に、ファイルを再インストールします。 • c は、ファイルが欠落している場合、またはインストール済みファイルの保存されているチェックサムが新しいファイルの値と一致しない場合に、ファイルを再インストールします。 • a は、すべてのファイルを強制的に再インストールします。 • u または m は、必要なすべてのユーザー・レジストリーを再書き込みします。 • s は、既存のショートカットを上書きします。 • v は、アプリケーションをソースから実行して、ローカル・インストール・パッケージを再度キャッシュに入れます。
/a *package*	/a オプションにより、管理者権限を持つユーザーは製品をネットワーク上にインストールできます。
/x *package* または *product code*	/x オプションは、製品をアンインストールします。

表 15. (続き)

パラメーター	説明
/L [i|w|e|a|r |u|c|m|p|v|+] *log file*	/L オプションを使用して作成すると、ログ・ファイルへのパスが指定されます。以下のフラグは、ログ・ファイルに記録する情報を示しています。 • i は、状況メッセージをログに記録します • w は、致命的でない警告メッセージをログに記録します • e は、すべてのエラー・メッセージをログに記録します • a は、アクション・シーケンスの開始をログに記録します • r は、アクション固有のレコードをログに記録します • u は、ユーザー要求をログに記録します • c は、初期ユーザー・インターフェース・パラメーターをログに記録します • m は、メモリー不足メッセージをログに記録します • p は、端末設定をログに記録します • v は、冗長出力設定をログに記録します • + は、既存ファイルに付加します • * は、すべての情報を (冗長出力設定を除いて) ログに記録できるワイルドカード文字です
/q [n|b|r|f]	/q オプションを以下のフラグと併用して、ユーザー・インターフェース・レベルを設定します。 • q または qn は、ユーザー・インターフェースを作成しません。 • qb は、基本ユーザー・インターフェースを作成します。 下記のユーザー・インターフェース設定により、インストール終了時にモーダル・ダイアログ・ボックスが表示されます。 • qr は、縮小ユーザー・インターフェースを表示します。 • qf は、完全なユーザー・インターフェースを表示します。 • qn+ は、ユーザー・インターフェースを表示しません。 • qb+ は、基本ユーザー・インターフェースを表示します。
/? または /h	いずれかのコマンドにより、Windows インストーラの著作権情報が表示されます。
TRANSFORMS	TRANSFORMS コマンド・ライン・パラメーターを使用して、基本パッケージに適用する変換を指定します。変換のコマンド・ライン呼び出しは、以下のようになります。 `msiexec /i "C:¥WindowsFolder¥Profiles¥UserName¥Personal¥MySetups¥Your Project Name¥Trial Version¥My Release-1¥DiskImages¥Disk1¥ProductName.msi" TRANSFORMS="New Transform 1.mst"` 複数の変換をセミコロンで分離できます。そのため、Windows インストーラ・サービスが誤って解釈しないように、変換の名前にセミコロンを使用しないことをお勧めします。

表 15. (続き)

パラメーター	説明
Properties	すべての共通プロパティはコマンド・ラインで設定または変更できます。共通プロパティはすべて大文字であるため、専用プロパティと区別されます。たとえば、 COMPANYNAME は共通プロパティです。 コマンド・ラインからプロパティを設定するには、次の構文を使用します。 PROPERTY=VALUE COMPANYNAME の値を変更するには、次のように入力します。 `msiexec /i "C:¥WindowsFolder¥Profiles¥UserName ¥Personal¥MySetups¥Your Project Name¥Trial Version¥My Release-1¥DiskImages¥Disk1¥ProductName.msi" COMPANYNAME="InstallShield"`

標準 Windows インストーラの共通プロパティ

Windows インストーラには、一連の標準組み込み共通プロパティがあります。これらのプロパティをコマンド・ラインで設定して、インストール時の特定の動作を指定することができます。以下に、コマンド・ラインで使用される最も一般的な共通プロパティについて説明します。より詳細な資料は、 Microsoft Web サイト (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_properties.asp) で入手できます。

表 16 に、一般に使用される Windows インストーラのプロパティを示します。

表 16.

プロパティ	説明
TARGETDIR	インストール用の宛先のルート・ディレクトリーを指定します。管理用インストールの場合、このプロパティは、インストール・パッケージのコピー先です。
ARPAUTHORIZEDCDFPREFIX	アプリケーションの更新チャネルの URL。
ARPCOMMENTS	「コントロール パネル」の「プログラムの追加と削除」に「コメント」を提供します。
ARPCONTACT	「コントロール パネル」の「プログラムの追加と削除」に「連絡先」を提供します。
ARPINSTALLLOCATION	アプリケーションの 1 次フォルダーへの完全修飾パス。
ARPNOMODIFY	製品を変更する機能を使用不可にします。
ARPNOREMOVE	製品を削除する機能を使用不可にします。
ARPNOREPAIR	「プログラム」ウィザードの「修復」ボタンを使用不可にします。
ARPPRODUCTICON	インストール・パッケージの基本アイコンを指定します。
ARPREADME	「コントロール パネル」の「プログラムの追加と削除」に README を提供します。
ARPSIZE	アプリケーションの推定サイズ (KB)。

表 16. (続き)

プロパティ	説明
ARPSYSTEMCOMPONENT	「プログラムの追加と削除」のリストにアプリケーションを表示しないようにします。
ARPURLINFOABOUT	アプリケーションのホーム・ページの URL。
ARPURLUPDATEINFO	アプリケーション更新情報の URL。
REBOOT	REBOOT プロパティにより、システムの再起動を促す特定のプロンプトが抑止されます。管理者は通常、一連のインストールを行う際にこのプロパティを使用して、複数の製品を同時にインストールし、最後に一度だけ再起動します。インストール終了時の再起動を使用不可にするには、REBOOT=”R” と設定します。
INSTALLDIR	このプロパティには、ご使用の機能とコンポーネント内のファイルのデフォルトの宛先フォルダーが含まれます。

Rescue and Recovery のカスタム共通プロパティ

Rescue and Recovery プログラムのインストール・パッケージには、一連のカスタム共通プロパティが含まれています。インストールを実行する際は、これらのプロパティをコマンド・ラインで設定することができます。使用可能なカスタム共通プロパティは、以下のとおりです。

表 17.

プロパティ	説明
PDA	ワークスペースをインストールするかどうかを指定します。デフォルト値は 1 です。 1 はワークスペースをインストールし、0 はワークスペースをインストールしません。注: この設定は、いずれかのバージョンのワークスペースがすでに存在している場合は使用されません。
CIMPROVIDER	CIM プロバイダー・コンポーネントをインストールするかどうかを指定します。デフォルトはこのコンポーネントをインストールしません。このコンポーネントをインストールする場合は、コマンド・ラインで CIMPROIVIDER=1 を指定します。
EMULATIONMODE	TPM が存在する場合でも、強制的にエミュレーション・モードでインストールを実行するように指定します。エミュレーション・モードでインストールするには、コマンド・ラインで EMULATIONMODE=1 と設定します。

表 17. (続き)

プロパティ	説明
HALTIFCSS54X	CSS 5.4X がインストール済みで、インストールがサイレント・モードで実行されている場合、デフォルトではインストールをエミュレーション・モードで進めます。インストールをサイレント・モードで実行するときは、HALTIFCSS54X=1 プロパティを使用して、CSS 5.4X がインストール済みの場合にインストールを停止します。
HALTIFTPMDISABLED	TPM が使用不可状態で、インストールがサイレント・モードで実行されている場合、デフォルトではインストールをエミュレーション・モードで進めます。インストールをサイレント・モードで実行するときは、HALTIFTPMDISABLED=1 プロパティを使用して、 TPM が使用不可の場合にインストールを停止します。
ENABLETPM	インストールで TPM を使用可能にできないようにするには、コマンド・ラインで ENABLETPM=0 を設定します。
NOCSS	Client Security Solution とそのサブ機能がインストールされないようにするには、コマンド・ラインで NOCSS=1 を設定します。このプロパティは、サイレント・インストールでの使用を想定したものですが、 UI インストールでも使用できます。UI インストールでは、CSS 機能はカスタム・セットアップ画面には表示されません。
NOPRVDISK	SafeGuard PrivateDisk の機能がインストールされないようにするには、コマンド・ラインで NOPRVDISK=1 を設定します。このプロパティは、サイレント・インストールでの使用を想定したものですが、 UI インストールでも使用できます。UI インストールでは、SafeGuard PrivateDisk 機能はカスタム・セットアップ画面には表示されません。
NOPWMANAGER	Password Manager の機能がインストールされないようにするには、コマンド・ラインで NOPWMANAGER=1 を設定します。このプロパティは、サイレント・インストールでの使用を想定したものですが、 UI インストールでも使用できます。UI インストールでは、Password Manager 機能はカスタム・セットアップ画面には表示されません。

表 17. (続き)

プロパティ	説明
NOCSSWIZARD	管理者がログオンし、まだ登録していないときに CSS ウィザードが表示されないようにするには、コマンド・ラインで NOCSSWIZARD=1 を設定します。このプロパティは、CSS はインストールしても、システムの実際の構成は後でスクリプトを使用して行う場合に適しています。
CSS_CONFIG_SCRIPT	ユーザーがインストールを完了し、再起動した後に構成ファイルを実行するには、CSS_CONFIG_SCRIPT=”*filename*” または “*filename password*” を設定します。
SUPERVISORPW	コマンド・ラインで SUPERVISORPW=”*password*” と設定すると、スーパーバイザー・パスワードが提供され、サイレント・インストール・モードでも非サイレント・インストール・モードでも、チップが使用可能になります。チップが使用不可で、インストールをサイレント・モードで実行する場合、チップを使用可能にするには正しいスーパーバイザー・パスワードを入力する必要があります。パスワードが正しくないと、チップは使用可能になりません。

ログ・ファイルのインストール

ログ・ファイル rrinstall30.log は、setup.exe でセットアップが起動すると (メインのインストール exe をダブルクリックするか、パラメーターなしでメインの exe を実行するか、msi を解凍して setup.exe を実行します)、%temp% ディレクトリーに作成されます。このファイルには、インストール問題のデバッグに使用できるログ・メッセージが含まれています。 このログ・ファイルは、msi パッケージからセットアップを直接実行している場合には作成されません。このログ・ファイルには、「プログラムの追加と削除」から実行されるアクションが含まれています。すべての MSI アクションのログ・ファイルを作成するには、レジストリー内のログ・ポリシーを使用可能にすることができます。これを行うには、次の値を作成します。

```
[HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥Windows¥Installer]
"Logging"="voicewarmup"
```

インストールの例

次の表は、setup.exe を使用した例です。

表 18.

説明	例
サイレント・インストール (再起動なし)	`setup.exe /s /v"/qn REBOOT="R""`
管理用インストール	`setup.exe /a`
管理用のサイレント・インストール (解凍先を指定)	`setup.exe /a /s /v"/qn TARGETDIR="F:¥TVTRR""`
サイレント・アンインストール setup.exe /s /x /v/qn	`setup.exe /s /x /v/qn`

表 18. (続き)

説明	例
再起動なしのインストールで、temp フォルダーにインストール・ログを作成	`setup.exe /v"REBOOT="R" /L*v %temp%¥rrinstall30.log"`
ワークスペースをインストールしないインストール setup.exe /vPDA=0	`setup.exe /vPDA=0`

次の表に、Rescue and Recovery/Client Security Solution.msi を使用したインストールの例を示します。

表 19.

説明	例
インストール	msiexec /i “C:¥TVTRR¥Rescue and Recovery/Client Security Solution.msi”
サイレント・インストール (再起動なし)	msiexec /i “C:¥TVTRR¥Rescue and Recovery/Client Security Solution.msi” /qn REBOOT=”R”
サイレント・アンインストール	msiexec /x “C:¥TVTRR¥Rescue and Recovery/Client Security Solution.msi” /qn
ワークスペースをインストールしないインストール	msiexec /i “C:¥TVTRR¥Rescue and Recovery/Client Security Solution.msi” PDA=0

Rescue and Recovery のディスク・イメージへの組み込み

サード・パーティー製複製ツールを使用して、Rescue and Recovery が組み込まれたディスク・イメージを作成することができます。本デプロイメント・ガイドでは、PowerQuest および Ghost について基本的な情報を記載しています。本書では、読者がイメージ作成ツールを使い慣れていること、およびイメージ作成に必要なその他のオプションを理解していることを前提としています。

注: イメージを作成する場合、マスター・ブート・レコードを取り込む必要があります。マスター・ブート・レコードは、Rescue and Recovery ワークスペースが正常に機能する上で重要です。

PowerQuest Drive Image ベースのツールの使用

PowerQuest DeployCenter ツール PQIMGCTR が X:¥PQ にインストールされていることを前提として、次のスクリプトにより Rescue and Recovery がインストールされたイメージの作成とデプロイメントを行うことができます。

最小スクリプト・ファイル

表 20. X:¥PQ¥RRUSAVE.TXT

スクリプト言語	結果
`SELECT DRIVE 1`	最初のハードディスク・ドライブを選択する

表 20. X:¥PQ¥RRUSAVE.TXT (続き)

スクリプト言語	結果
`SELECT PARTITION ALL` (タイプ 12 区画またはイメージ内に複数の区画がある場合に必要。)	すべての区画を選択する
Store with compression high	イメージを保管する

表 21. X:¥PQ¥RRDEPLY.TXT

スクリプト言語	結果
`SELECT DRIVE 1`	最初のハードディスク・ドライブを選択する
`DELETE ALL`	すべての区画を削除する
`SELECT FREESPACE FIRST`	最初の空き領域を選択する
`SELECT IMAGE ALL`	イメージのすべての区画を選択する
`RESTORE`	イメージを復元する

イメージ作成

表 22. X:¥PQ¥PQIMGCTR / CMD=X:¥PQ¥RRUSAVE.TXT /MBI=1 / IMG=X:¥IMAGE.PQI

スクリプト言語	結果
`SELECT DRIVE 1`	最初のハードディスク・ドライブを選択する
`X:¥PQ¥PQIMGCTR`	PQIMGCTR のパス
`/CMD=X:¥PQ¥RRUSAVE.TXT`	PowerQuest スクリプト・ファイル
`/MBI=1`	Rescue and Recovery Boot Manager を取り込む
`/IMG=X:¥IMAGE.PQI`	イメージ・ファイルのパス

イメージ・デプロイメント

表 23. X:¥PQ¥PQIMGCTR / CMD=X:¥PQ¥RRDEPLY.TXT /MBI=1 / IMG=X:¥IMAGE.PQI

スクリプト言語	結果
`SELECT DRIVE 1`	最初のハードディスク・ドライブを選択する
`X:¥PQ¥PQIMGCTR`	PQIMGCTR のパス
`/CMD=X:¥PQ¥RRDEPLY.TXT`	PowerQuest スクリプト・ファイル
`/MBR=1`	Rescue and Recovery Boot Manager を復元する
`/IMG=X:¥IMAGE.PQI`	イメージ・ファイルのパス

Symantec Ghost ベースのツール

Ghost イメージを作成する場合、コマンド・ライン・スイッチ (GHOST.INI ファイルに組み込まれている) `-ib` を使用して Rescue and Recovery Boot Manager を取り

込む必要があります。また、イメージにはディスク全体およびすべての区画を取り込む必要があります。 Ghost について詳しくは、Symantec が提供している資料を参照してください。

Client Security Solution バージョン 6.0 のインストール・コンポーネント

Client Security Solution 6.0 のインストール・パッケージは、基本 MSI プロジェクトとして InstallShield 10.5 Premier を使用して開発されています。InstallShield 10.5 Basic MSI プロジェクトは、 Windows インストーラを使用して、アプリケーションをインストールします。これにより、管理者には、コマンド・ラインからのプロパティ値の設定などの、インストールをカスタマイズする多くの機能が提供されます。以下のセクションでは、 CSS 6.0 セットアップ・パッケージの使用および実行方法について説明します。詳しくは、以下の説明をすべてお読みください。

インストール・コンポーネント

CSS 6.0 のインストールは、単一の exe ファイル (約 20 MB) で構成されています。これは、インストール・プロジェクト・ソースから作成された setup.exe です。setup.exe ファイルは、ビルド・プロセスで、プロジェクト ID、メディア・タイプ、ビルド・レベル、国別コード (この場合は常に US)、およびパッチ・コードを表す名前 (たとえば 169ZIS1001US00.exe) に変更されます。これは、インストール・ソース・ファイルを解凍し、 Windows インストーラを使用してインストールを起動する自己解凍型インストール・パッケージです。このファイルには、インストール・ロジックと Windows アプリケーション・ファイルが含まれています。

標準的なインストール手順およびコマンド・ライン・パラメーター

Setup.exe では、以下に説明する一連のコマンド・ライン・パラメーターを使用できます。パラメーターを必要とするコマンド・ライン・オプションは、オプションとパラメーターの間にスペースを入れずに指定する必要があります。以下に例を示します。

```
Setup.exe /s /v"/qn REBOOT="R""
```

は有効ですが、

```
Setup.exe /s /v"/qn REBOOT="R""
```

は無効です。オプションのパラメーターは、そのパラメーターにスペースが含まれている場合に限り、引用符で囲む必要があります。

注: インストールを単独で実行すると (パラメーターを指定せずに setup.exe だけを実行すると)、デフォルトでは、インストール終了時にユーザーに再起動を促すプロンプトが出されます。プログラムを正しく機能させるには、再起動する必要があります。上記および例のセクションで示すように、サイレント・インストールではコマンド・ライン・パラメーターを使用して再起動を遅らせることができます。

以下のパラメーターとその説明は、InstallShield Developer ヘルプ文書から直接引用しています。基本 MSI プロジェクトに適用されないパラメーターは、除かれています。

表 24.

パラメーター	説明
/a ： 管理用インストール	/a スイッチを指定すると、Setup.exe で管理用インストールが実行されます。管理用インストールは、データ・ファイルをユーザーが指定したディレクトリーにコピー (および解凍) しますが、ショートカットの作成、COM サーバーの登録、アンインストール・ログの作成は行いません。
/x ： アンインストール・モード	/x スイッチを指定すると、Setup.exe は以前にインストールした製品をアンインストールします。
/s ： サイレント・モード	コマンド Setup.exe /s を実行すると、基本 MSI インストール・プログラム用の Setup.exe 初期設定ウィンドウは表示されず、応答ファイルは読み取られません。基本 MSI プロジェクトでは、サイレント・インストールの場合、応答ファイルは作成も使用もされません。基本 MSI 製品をサイレントで実行するには、コマンド・ライン Setup.exe /s /v/qn を実行します。 (基本 MSI のサイレント・インストールの共通プロパティ値を指定する場合は、 Setup.exe /s /v″/qn INSTALLDIR=D:¥Destination″ などのコマンドを使用できます。)
/v ： Msiexec への引数の受け渡し	/v 引数を使用して、 Msiexec.exe にコマンド・ライン・スイッチと共通プロパティの値を渡します。
/L ： 言語のセットアップ	ユーザーは、/L スイッチと 10 進言語 ID を使用して、複数言語インストール・プログラムで使用する言語を指定します。たとえば、ドイツ語を指定するコマンドは Setup.exe /L1031 です。注: 表 25 に記載されているすべての言語のインストールがサポートされているわけではありません。
/w ： 待機	基本 MSI プロジェクトで引数 /w を指定すると、Setup.exe は、インストールが完了するのを待ってから終了します。バッチ・ファイルで /w オプションを使用すると、Setup.exe のコマンド・ライン引数全体を start /WAIT で開始することができます。正しくフォーマットされたコマンドの使用例は、次のとおりです。 `start /WAIT setup.exe /w`

表 25.

言語	ID
アラビア語 (サウジアラビア)	1025

表 25. (続き)

言語	ID
バスク語	1069
ブルガリア語	1026
カタロニア語	1027
中国語 (簡体字)	2052
中国語 (繁体字)	1028
クロアチア語	1050
チェコ語	1029
デンマーク語	1030
オランダ語 (標準)	1043
英語	1033
フィンランド語	1035
カナダ・フランス語	3084
フランス語	1036
ドイツ語	1031
ギリシャ語	1032
ヘブライ語	1037
ハンガリー語	1038
インドネシア語	1057
イタリア語	1040
日本語	1041
韓国語	1042
ノルウェー語 (ブークモール)	1044
ポーランド語	1045
ポルトガル語 (ブラジル)	1046
ポルトガル語 (標準)	2070
ルーマニア語	1048
ロシア語	1049
スロバキア語	1051
スロベニア語	1060
スペイン語	1034
スウェーデン語	1053
タイ語	1054
トルコ語	1055

管理用インストールの手順およびコマンド・ライン・パラメーター

Windows インストーラは、ワークグループによる使用またはカスタマイズのために、アプリケーションまたは製品のネットワークへの管理用インストールを実行できます。Rescue and Recovery/Client Security Solution インストール・パッケージの場合、管理用インストールによりインストール・ソース・ファイルが指定された場

所に解凍されます。管理用インストールを実行するには、セットアップ・パッケージをコマンド・ラインから /a パラメーターを使用して実行します。

```
Setup.exe /a
```

管理用インストールを実行すると、管理者にセットアップ・ファイルの解凍先を指定するようプロンプトを出す一連のダイアログ画面が表示されます。管理者に示されるデフォルトの解凍先は C:¥ です。 C: 以外のドライブ (他のローカル・ドライブやマップされたネットワーク・ドライブなど) の新しい場所を選択することもできます。新しいディレクトリーも、この手順で作成できます。

管理用インストールをサイレント・インストールで実行する場合、解凍先の場所を指定するために、コマンド・ラインで次のように共通プロパティ TARGETDIR を設定することができます。

```
Setup.exe /s /v"/qn TARGETDIR=F:¥TVTRR"
```

管理用インストールが完了した後、管理者はソース・ファイルをカスタマイズ (たとえば、設定値を tvt.txt に追加) することができます。カスタマイズ後に解凍したソースからインストールするには、ユーザーはコマンド・ラインで msiexec.exe を実行し、解凍された msi ファイルの名前を引き渡します。次のセクションでは、msiexec で有効なコマンド・ライン・パラメーターと、その使用方法を説明します。共通プロパティは、msiexec コマンド・ライン呼び出しで直接設定することもできます。

MsiExec.exe コマンド・ライン・パラメーター

MsiExec.exe は、Windows インストーラの実行可能プログラムで、インストール・パッケージを解釈し、製品をターゲット・システムにインストールするために使用されます。

```
msiexec. /i "C:WindowsFolder/Profiles¥UserName¥Persona¥MySetups¥project name
  ¥product configuration¥release name¥DiskImages¥Disk1¥product name.msi
```

次の表で、MsiExec.exe コマンド・ライン・パラメーターについて詳しく説明します。この表は、Windows インストーラに関する Microsoft Platform SDK 文書からの引用です。

表 26.

パラメーター	説明
/i *package* または *product code*	たとえば、Othello という名称の製品をインストールする場合、以下のように行います。 `msiexec /i "C:¥WindowsFolder¥Profiles¥UserName¥ Personal¥MySetups¥Othello¥Trial Version¥Release ¥DiskImages¥Disk1¥Othello Beta.msi"` 製品コードとは、製品のプロジェクト・ビューの製品コード・プロパティで自動生成される GUID のことです。

表 26. (続き)

パラメーター	説明
f [p|o|e|d|c|a|u|m|s|v] *package* または *product code*	インストール時に /f オプションを指定すると、欠落または破損したファイルが修復または再インストールされます。 たとえば、すべてのファイルを強制的に再インストールするには、次の構文を使用します。 `msiexec /fa "C:¥WindowsFolder¥Profiles¥UserName¥ Personal¥MySetups¥Othello¥Trial Version¥Release ¥DiskImages¥Disk1¥Othello Beta.msi"` 以下のフラグを結合することができます。 • p は、欠落したファイルを再インストールします。 • o は、ファイルが欠落している場合、またはユーザーのシステムに存在するファイルのバージョンが古い場合に、そのファイルを再インストールします。 • e は、ファイルが欠落している場合、またはユーザーのシステム上に同等のファイルまたは旧バージョンのファイルが存在する場合に、ファイルを再インストールします。 • c は、ファイルが欠落している場合、またはインストール済みファイルの保存されているチェックサムが新しいファイルの値と一致しない場合に、ファイルを再インストールします。 • a は、すべてのファイルを強制的に再インストールします。 • u または m は、必要なすべてのユーザー・レジストリーを再書き込みします。 • s は、既存のショートカットを上書きします。 • v は、アプリケーションをソースから実行して、ローカル・インストール・パッケージを再度キャッシュに入れます。
/a *package*	/a オプションにより、管理者権限を持つユーザーは製品をネットワーク上にインストールできます。
/x *package* または *product code*	/x オプションは、製品をアンインストールします。

表 26. (続き)

パラメーター	説明
/L [i|w|e|a|r |u|c|m|p|v|+] *log file*	/L オプションを使用して作成すると、ログ・ファイルへのパスが指定されます。以下のフラグは、ログ・ファイルに記録する情報を示しています。 • i は、状況メッセージをログに記録します • w は、致命的でない警告メッセージをログに記録します • e は、すべてのエラー・メッセージをログに記録します • a は、アクション・シーケンスの開始をログに記録します • r は、アクション固有のレコードをログに記録します • u は、ユーザー要求をログに記録します • c は、初期ユーザー・インターフェース・パラメーターをログに記録します • m は、メモリー不足メッセージをログに記録します • p は、端末設定をログに記録します • v は、冗長出力設定をログに記録します • + は、既存ファイルに付加します • * は、すべての情報を (冗長出力設定を除いて) ログに記録できるワイルドカード文字です
/q [n|b|r|f]	/q オプションを以下のフラグと併用して、ユーザー・インターフェース・レベルを設定します。 • q または qn は、ユーザー・インターフェースを作成しません。 • qb は、基本ユーザー・インターフェースを作成します。 下記のユーザー・インターフェース設定により、インストール終了時にモーダル・ダイアログ・ボックスが表示されます。 • qr は、縮小ユーザー・インターフェースを表示します。 • qf は、完全なユーザー・インターフェースを表示します。 • qn+ は、ユーザー・インターフェースを表示しません。 • qb+ は、基本ユーザー・インターフェースを表示します。
/? または /h	いずれかのコマンドにより、Windows インストーラの著作権情報が表示されます。

表 26. (続き)

パラメーター	説明
TRANSFORMS	TRANSFORMS コマンド・ライン・パラメーターを使用して、基本パッケージに適用される変換を指定します。変換のコマンド・ライン呼び出しは、以下のようになります。 `msiexec /i "C:¥WindowsFolder¥Profiles¥UserName¥ Personal¥MySetups¥Your Project Name¥Trial Version ¥My Release-1¥DiskImages¥Disk1¥ProductName.msi" TRANSFORMS="New Transform 1.mst"` 複数の変換をセミコロンで分離できます。そのため、Windows インストーラ・サービスが誤って解釈しないように、変換の名前にセミコロンを使用しないことをお勧めします。
Properties	すべての共通プロパティはコマンド・ラインで設定または変更できます。共通プロパティはすべて大文字であるため、専用プロパティと区別されます。たとえば、COMPANYNAME は共通プロパティです。 コマンド・ラインからプロパティを設定するには、次の構文を使用します。 PROPERTY=VALUE COMPANYNAME の値を変更するには、次のように入力します。 `msiexec /i "C:¥WindowsFolder¥Profiles¥UserName ¥Personal¥MySetups¥Your Project Name¥Trial Version¥My Release-1¥DiskImages¥Disk1¥ProductName.msi" COMPANYNAME="InstallShield"`

標準 Windows インストーラの共通プロパティ

Windows インストーラには、一連の標準組み込み共通プロパティがあります。これらのプロパティをコマンド・ラインで設定して、インストール時の特定の動作を指定することができます。以下に、コマンド・ラインで使用される最も一般的な共通プロパティについて説明します。より詳しい文書が、Microsoft の Web サイト (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_properties.asp) で入手できます。

表 27 に、一般に使用される Windows インストーラのプロパティを示します。

表 27.

プロパティ	説明
TARGETDIR	インストール用の宛先のルート・ディレクトリーを指定します。管理用インストールの場合、このプロパティは、インストール・パッケージのコピー先です。
ARPAUTHORIZEDCDFPREFIX	アプリケーションの更新チャネルの URL。
ARPCOMMENTS	「コントロール パネル」の「プログラムの追加と削除」に「コメント」を提供します。
ARPCONTACT	「コントロール パネル」の「プログラムの追加と削除」に「連絡先」を提供します。

表 27. (続き)

プロパティ	説明
ARPINSTALLLOCATION	アプリケーションの 1 次フォルダーへの完全修飾パス。
ARPNOMODIFY	製品を変更する機能を使用不可にします。
ARPNOREMOVE	製品を削除する機能を使用不可にします。
ARPNOREPAIR	「プログラム」ウィザードの「修復」ボタンを使用不可にします。
ARPPRODUCTICON	インストール・パッケージの基本アイコンを指定します。
ARPREADME	「コントロール パネル」の「プログラムの追加と削除」で README を提供します。
ARPSIZE	アプリケーションの推定サイズ (KB)。
ARPSYSTEMCOMPONENT	「プログラムの追加と削除」のリストにアプリケーションを表示しないようにします。
ARPURLINFOABOUT	アプリケーションのホーム・ページの URL。
ARPURLUPDATEINFO	アプリケーション更新情報の URL。
REBOOT	REBOOT プロパティにより、システムの再起動を促す特定のプロンプトが抑止されます。管理者は通常、一連のインストールを行う際にこのプロパティを使用して、複数の製品を同時にインストールし、最後に一度だけ再起動します。インストール終了時の再起動を使用不可にするには、REBOOT=”R” と設定します。
INSTALLDIR	このプロパティには、ご使用の機能とコンポーネント内のファイルのデフォルトの宛先フォルダーが含まれます。

Client Security Software カスタム共通プロパティ

Client Security Software プログラムのインストール・パッケージには、インストールの実行時にコマンド・ラインに設定できる、一連のカスタム共通プロパティが含まれています。使用可能なカスタム共通プロパティは、以下のとおりです。

表 28.

プロパティ	説明
EMULATIONMODE	TPM が存在する場合でも、強制的にエミュレーション・モードでインストールを実行するように指定します。エミュレーション・モードでインストールするには、コマンド・ラインで EMULATIONMODE=1 と設定します。

表 28. (続き)

プロパティ	説明
HALTIFTPMDISABLED	TPM が使用不可状態で、インストールがサイレント・モードで実行されている場合、デフォルトではインストールをエミュレーション・モードで進めます。インストールをサイレント・モードで実行するときは、HALTIFTPMDISABLED=1 プロパティを使用して、 TPM が使用不可の場合にインストールを停止します。
ENABLETPM	インストールで TPM を使用可能にできないようにするには、コマンド・ラインで ENABLETPM=0 を設定します。
NOPRVDISK	SafeGuard PrivateDisk の機能がインストールされないようにするには、コマンド・ラインで NOPRVDISK=1 を設定します。このプロパティは、サイレント・インストールでの使用を想定したものですが、 UI インストールでも使用できます。UI インストールでは、SafeGuard PrivateDisk 機能はカスタム・セットアップ画面には表示されません。
NOPWMANAGER	Password Manager の機能がインストールされないようにするには、コマンド・ラインで NOPWMANAGER=1 を設定します。このプロパティは、サイレント・インストールでの使用を想定したものですが、 UI インストールでも使用できます。UI インストールでは、Password Manager 機能はカスタム・セットアップ画面には表示されません。
NOCSSWIZARD	管理者がログオンし、まだ登録していないときに CSS ウィザードが表示されないようにするには、コマンド・ラインで NOCSSWIZARD=1 を設定します。このプロパティは、CSS はインストールしても、システムの実際の構成は後でスクリプトを使用して行う場合に適しています。
CSS_CONFIG_SCRIPT	ユーザーがインストールを完了し、再起動した後に構成ファイルを実行するには、CSS_CONFIG_SCRIPT=”*filename*” または “*filename password*” を設定します。

表 28. (続き)

プロパティ	説明
SUPERVISORPW	コマンド・ラインで SUPERVISORPW=”*password*” と設定すると、スーパーバイザー・パスワードが提供され、サイレント・インストール・モードでも非サイレント・インストール・モードでも、チップが使用可能になります。チップが使用不可で、インストールをサイレント・モードで実行する場合、チップを使用可能にするには正しいスーパーバイザー・パスワードを入力する必要があります。パスワードが正しくないと、チップは使用可能になりません。

ログ・ファイルのインストール

setup.exe によってセットアップが開始されると (メインのインストール exe をダブルクリックする、パラメーターを指定せずにメインの exe を実行する、msi を解凍して setup.exe を実行する、のいずれかの方法で)、 %temp% フォルダーにログ・ファイル cssinstall60.log が作成されます。このファイルには、インストール問題のデバッグに使用できるログ・メッセージが含まれています。 このログ・ファイルは、msi パッケージから直接セットアップを実行する場合は作成されません。「プログラムの追加と削除」から実行するアクションがこれに該当します。すべての MSI アクションのログ・ファイルを作成するには、レジストリー内のログ・ポリシーを使用可能にすることができます。そのためには、次の値を作成します。

```
[HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥Windows¥Installer]
"Logging"="voicewarmup"
```

インストールの例

次の表は、setup.exe を使用した例です。

表 29.

説明	例
サイレント・インストール (再起動なし)	`setup.exe /s /v"/qn REBOOT="R""`
管理用インストール	`setup.exe /a`
管理用のサイレント・インストール (解凍先を指定)	`setup.exe /a /s /v"/qn TARGETDIR="F:¥CSS60""`
サイレント・アンインストール setup.exe /s /x /v/qn	`setup.exe /s /x /v/qn`
再起動なしのインストールで、temp フォルダーにインストール・ログを作成	`setup.exe /v"REBOOT="R" /L*v %temp%¥cssinstall60.log"`
ワークスペースをインストールしないインストール setup.exe /vPDA=0	`setup.exe /vPDA=0`

次の表は、Client Security Solution.msi を使用したインストールの例です。

表 30.

説明	例
インストール	`msiexec /i "C:¥CSS60¥Client Security Solution.msi"`

表 30. (続き)

説明	例
サイレント・インストール (再起動なし)	`msiexec /i "C:¥CSS60¥Client Security Solution.msi" /qn REBOOT="R"`
サイレント・アンインストール	`msiexec /x "C:¥CSS60¥Client Security Solution.msi" /qn`

System Migration Assistant のインストール

System Migration Assistant のインストール手順は、「*System Migration Assistant ユーザーズ・ガイド*」に記載されています。

指紋認証ユーティリティーのインストール

指紋認証ユーティリティー・プログラムの setup.exe ファイルは、開始時に以下のパラメーターを指定できます。

サイレント・インストール

指紋認証ユーティリティーもサイレント・インストールが可能です。CD-ROM ドライブの Install フォルダーで、 Setup.exe を実行してください。

このときの構文は次のようになります。

```
Setup.exe PROPERTY=VALUE /q /i
```

ここで、*q* はサイレント・インストール、*i* はインストールを表します。例:

```
Setup.exe INSTALLDIR="F:¥Program Files¥IBM fingerprint software" /q /i
```

このソフトウェアをアンインストールするには、代わりに /x パラメーターを使用します。

```
Setup.exe INSTALLDIR="F:¥Program Files¥IBM fingerprint software" /q /x
```

SMS インストール

SMS インストールもサポートされています。SMS 管理者コンソールを開き、新規パッケージを作成して標準的なパッケージ・プロパティを設定します。そのパッケージを開き、「プログラム」項目で「新規プログラム」を選択します。コマンド・ラインに次のように入力します。

```
Setup.exe /m yourmiffilename /q /i
```

サイレント・インストールの場合と同じパラメーターが使用できます。

Setup では、通常はインストール・プロセス終了時に再起動します。インストール中は再起動せず、後で (さらにいくつかのプログラムをインストールしてから) 再起動する場合は、プロパティ・リストに REBOOT=″ReallySuppress″ を追加します。

オプション

指紋認証ユーティリティーでは以下のオプションがサポートされています。

表 31.

パラメーター	説明
CTRLONCE	コントロール・センターを表示するのに一度だけ使用されます。デフォルトは 0 です。
CTLCNTR	始動時にコントロール・センターを実行するのに使用されます。デフォルトは、1 です。
DEFFUS	• 0 = Fast User Switching (FUS) 設定を使用しません。 • 1 = FUS 設定の使用を試みます。 デフォルトは 0 です。
INSTALLDIR	指紋認証ユーティリティーのデフォルトのインストール・ディレクトリー
OEM	• 0 = サーバー・パスポート/サーバー認証のインストールをサポート • 1 = スタンドアロン PC モードのみ (ローカル・パスポート)
PASSPORT	インストール時に設定されるデフォルトのパスポート・タイプ • 1 = デフォルト - ローカル・パスポート • 2 = サーバー・パスポート デフォルトは、1 です。
SECURITY	• 1 - = セキュア・モードのインストールをサポート • 0 = インストールしない。便利モードのみ存在
SHORTCUTFOLDER	「スタート」メニューのショートカット・フォルダーのデフォルト名
REBOOT	ReallySuppress に設定すると、インストール中は、プロンプトを含むすべての再起動を行わないようにできます。

インストールするソフトウェアのシナリオ

表 32.

インストールするソフトウェア	注
Client Security Software バージョン 5.4x	CSS で Rescue and Recovery との共存をサポートしているのは、このバージョンのみです。

表 32. (続き)

インストールするソフトウェア	注
Rescue and Recovery バージョン 3.0 のみ	• 製品のフルインストールによってインストールします (CSS は選択解除)。 • Client Security Solution の一部のコア・コンポーネントは RnR 単独インストールでもインストールされ、 TPM によるバックアップの暗号化と PDA マスター・パスワード構成をサポートします。
Client Security Solution バージョン 6.0 スタンドアロン	• これは、個別のインストール・パッケージです。 • 製品をフルインストールし、Rescue and Recovery を選択解除して Client Security Solution のみを入れることはできません。 • CSS コンポーネント (Private Disk と Password Manager) はオプションです。
Rescue and Recovery バージョン 3.0 および Client Security Solution バージョン 6.0	• デフォルトをプリロード - 通常の製品インストール • CSS コンポーネント • Private Disk と Password Manager はオプションのコンポーネントです。

ソフトウェアの状態変更

表 33.

インストール済みソフトウェア	使用したいソフトウェア	実行するプロセス	注	ビルド
Client Security Software バージョン 5.4x	Client Security Software 5.4x および Rescue and Recovery バージョン 3.0	• 製品をインストールします。 • Rescue and Recovery コンポーネントのみがインストールされます (カスタム構成画面は表示されません)。 • プロンプトが出たら、Client Security Software のインストールを保持するよう指示します。	• Rescue and Recovery 用の Client Security Software フックは、エミュレーション・モードで実行されます。 • このモードでは、Client Security Software によるマスター・パスワードのみが使用できます。	011

表 33. (続き)

インストール済みソフトウェア	使用したいソフトウェア	実行するプロセス	注	ビルド
Client Security Software	Client Security Solution 6.0	• Client Security Software 5.4x をアンインストールします。 • Client Security Solution 6.0 スタンドアロンをインストールします。	Client Security Software バージョン 5.4x に Client Security Solution バージョン 6.0 を上書きインストールすることは、許可されていません。ユーザーは、まず古い Client Security Software を削除するよう求められます。	011
Client Security Software	Rescue and Recovery バージョン 3.0 および Client Security Solution バージョン 6.0	• Client Security Software 5.4x をアンインストールします。 • 製品をインストールします。	Client Security Software バージョン 5.4x にこの製品を上書きインストールしようとすると、まず Client Security Software バージョン 5.4x を削除することを促すプロンプトが出されます。アンインストールせずにインストールを続行した場合は、 Rescue and Recovery だけがインストールされます。	011

表 34.

インストール済みソフトウェア	使用したいソフトウェア	実行するプロセス	注	ビルド
Rescue and Recovery バージョン 3.0	Client Security Software 5.4x および Rescue and Recovery バージョン 3.0	• Rescue and Recovery をアンインストールします。 • Client Security Software バージョン 5.4x をインストールします。 • 上記の説明に従って製品をインストールします。	• Client Security Software バージョン 5.4x は、他の製品がインストールされているとインストールできません。 • ローカル・バックアップは、Rescue and Recovery バージョン 3.0 のアンインストール時に削除されます。	011

表 34. (続き)

インストール済みソフトウェア	使用したいソフトウェア	実行するプロセス	注	ビルド
Rescue and Recovery バージョン 3.0	Client Security Solution 6.0	• Rescue and Recovery バージョン 3.0 をアンインストールします。 • Client Security Solution バージョン 6.0 スタンドアロンをインストールします。	• Rescue and Recovery バージョン 3.0 をアンインストールすると、ユーザー・ファイルと CSS レジストリー設定は削除されます。 • CSS によって保護されている Rescue and Recovery バージョン 3.0 のバックアップには、アクセスできなくなります。 • ローカル・バックアップは、Rescue and Recovery バージョン 3.0 のアンインストール時に削除されます。 • Client Security Software バージョン 6.0 スタンドアロンのインストールは、他の製品がインストールされていると許可されません。 • 「プログラムの追加と削除」の「変更」オプションでは、この場合は、 Client Security Solution の追加のみが許可されます。Rescue and Recovery は、「変更」オプションでは削除できません。	012
Rescue and Recovery バージョン 3.0	Rescue and Recovery バージョン 3.0 および Client Security Solution バージョン 6.0	• 「プログラムの追加と削除」から「変更」オプションを選択します。 • CSS および任意の追加コンポーネントを追加します。	• CSS を追加すると、ローカル・バックアップは削除されます。 • ユーザーは、Client Security Solution を追加する際、Client Security Solution の追加後に新しくバックアップを取るように注意されます。 • Client Security Solution の設定とデータ・ファイルは、Client Security Solution の追加時に削除されます。 • Client Security Solution バージョン 6.0 スタンドアロンのインストールは、他の製品がインストールされていると許可されません。	TBD

表 35.

インストール済みソフトウェア	使用したいソフトウェア	実行するプロセス	注	ビルド
Client Security Solution バージョン 6.0 スタンドアロン	Client Security Software 5.4x	• Client Security Solution バージョン 6.0 をアンインストールします。 • Client Security Software バージョン 5.4x をインストールします。	• Client Security Solution バージョン 5.4x は、他の製品がインストールされているとインストールできません。 • Client Security Solution バージョン 6.0 をアンインストールすると、データ・ファイルおよび設定の削除を促すプロンプトが出されます。ここで選択したオプションは、Client Security Software バージョン 5.4x の操作には影響を与えません。	011
Client Security Solution バージョン 6.0 スタンドアロン	Rescue and Recovery バージョン 3.0	• Client Security Solution バージョン 6.0 をアンインストールします。 • 製品をインストールし、Rescue and Recovery だけを選択します。	• Client Security Solution バージョン 6.0 をアンインストールすると、その Client Security Solution のユーザー・ファイルおよび設定の削除を促すプロンプトが出されます。 • Rescue and Recovery 3.0 をインストールすると、ユーザーに、既存の Client Security Solution ユーザー・ファイルおよび設定の削除を促すプロンプトが出されます。ユーザーがファイルを削除しない場合、インストールは取り消されます。	012

表 35. (続き)

インストール済みソフトウェア	使用したいソフトウェア	実行するプロセス	注	ビルド
Client Security Solution バージョン 6.0 スタンドアロン	Rescue and Recovery バージョン 3.0 および Client Security Solution バージョン 6.0	• 製品のインストールを実行します。 • Rescue and Recovery と Client Security Solution のオプションは選択解除できません。 • 以前にインストールされた Client Security Solution コンポーネント (Password Manager と Private Disk) がデフォルトで選択されていますが、これは解除することができます。以前にインストールされていないコンポーネントは、デフォルトでは選択されていませんが、選択することはできます。	• Client Security Solution バージョン 6.0 スタンドアロンは、バックグラウンドでアンインストールされます。 • Client Security Solution バージョン 6.0 のデータ・ファイルおよび設定は保持されます。 • エミュレーション/非エミュレーションの状態は保持されます。 • 製品のインストール完了後、Client Security Solution ウィザードが動作しないのは、 Client Security Solution が以前に構成されているためです。 • Client Security Solution によって Rescue and Recovery のバックアップを保護するためのオプションは、Rescue and Recovery GUI 経由で実行する必要があります。最後のインストール画面で再起動した後に、Rescue and Recovery GUI を実行するオプションがあります。 • 製品のインストール後は、「プログラムの追加と削除」のオプションとして、「削除」、「修復」、および「変更」が組み込まれます。 • インストール済みの Client Security Solution バージョン 6.0 は、インストールされる製品のバージョンと同等か、それ以下でなければなりません。そうでない場合、製品がインストールできないというメッセージが表示されます。	012

注:

1. ユーザーが Rescue and Recovery 3.0 をサイレント・インストールする場合、Client Security Solution のユーザー・ファイルおよび設定は、インストール時に自動的に削除されます。

2. このシナリオでは、製品 (Rescue and Recovery 3.0 および Client Security Solution 6.0) のインストール時に Password Manager と Private Disk を選択するか選択解除するかによって、インストール後のコンポーネントの最終状態が決まります。たとえば、Client Security Solution 6.0 と同時に Password Manager をインストールして、製品のインストール中にその選択を解除した場合、それは、インストールの完了後にはインストールされなくなります。製品 (Rescue and Recovery および Client Security Solution) のサイレント・インストールを実行する場合は、インストール・コマンドでそれぞれのプロパティ NOPRVDISK=1 または NOPWMANAGER=1 を設定しない限り、Password Manager も Private Disk もインストールされます。

表 36.

インストール済みソフトウェア	**使用したいソフトウェア**	**実行するプロセス**	**注**	**ビルド**
Rescue and Recovery バージョン 3.0 および Client Security Solution バージョン 6.0	Client Security Software 5.4x	• 製品をアンインストールします。 • Client Security Solution バージョン 5.4x をインストールします。	• Client Security Software バージョン 5.4x は、他の製品がインストールされているとインストールできません。 • この製品をアンインストールすると、データ・ファイルおよび設定の削除を促すプロンプトが出されます。ここで選択したオプションは、Client Security Software バージョン 5.4x の操作には影響を与えません。	011

表 36. (続き)

インストール済みソフトウェア	使用したいソフトウェア	実行するプロセス	注	ビルド
Rescue and Recovery バージョン 3.0 および Client Security Solution バージョン 6.0	Rescue and Recovery バージョン 3.0	• 「プログラムの追加と削除」から「変更」オプションを選択します。 • Client Security Solution を削除します。	• Client Security Solution を削除すると、ローカル・バックアップは削除されます。 • Client Security Solution をアンインストールすると、PrivateDisk および Password Manager が失われるという警告が出されます。 • Client Security Solution によって保護されている Rescue and Recovery バージョン 3.0 のバックアップには、アクセスできなくなります。 • Client Security Solution の設定およびデータ・ファイルは、「変更」によって Client Security Solution を削除すると削除されます。	TBD (ビルド 12 には含まれない)

表 36. (続き)

インストール済みソフトウェア	使用したいソフトウェア	実行するプロセス	注	ビルド
Rescue and Recovery バージョン 3.0 および Client Security Solution バージョン 6.0	Client Security Solution バージョン 6.0	• 製品をアンインストールします。 • アンインストールすると、Client Security Solution のファイルおよび設定の削除を促すプロンプトが出されます。ユーザーが既存の Client Security Solution 構成を維持したい場合は、これを保持することができます。 • Client Security Solution バージョン 6.0 スタンドアロンをインストールします。	• 製品をアンインストールします。 • アンインストールすると、Client Security Solution のファイルおよび設定の削除を促すプロンプトが出されます。ユーザーが既存の Client Security Solution 構成を維持したい場合は、これを保持することができます。 • Client Security Solution バージョン 6.0 スタンドアロンをインストールします。	012

注:

1. 「プログラムの追加と削除」、またはオリジナル・ソースのユーザー・インターフェースから Client Security Solution 6.0 をアンインストールすると、ユーザーには、CSS の設定およびデータ・ファイルの削除を促すプロンプトが出されます。コマンド・ラインからサイレント・アンインストールを実行する場合、デフォルトでは CSS の設定およびデータ・ファイルは削除されますが、アンインストール・コマンドでプロパティ NOCSSCLEANUP=1 を設定すると、このアクションをオーバーライドすることができます。
2. 「プログラムの追加と削除」、またはオリジナル・ソースのユーザー・インターフェースから製品 (Rescue and Recovery と Client Security Solution 6.0) をアンインストールすると、ユーザーには、Client Security Solution の設定およびデータ・ファイルの削除を促すプロンプトが出されます。コマンド・ラインからサイレント・アンインストールを実行する場合、デフォルトでは Client Security Solution の設定およびデータ・ファイルは削除されますが、アンインストール・コマンドでプロパティ NOCSSCLEANUP=1 を設定すると、このアクションをオーバーライドすることができます。

第 7 章 Antidote Delivery Manager のインフラストラクチャー

Antidote Delivery Manager は、管理者からの命令を各システムに配信し、ウィルスまたはワームに対抗するためのコマンドをサポートすることによって働きます。管理者は、各システムで望ましいアクションを含むスクリプトを用意します。リポジトリー機能は、スクリプトを数分間以内に PC に安全に配信し、コマンドを実行します。コマンドには、ネットワーク接続の制限、エンド・ユーザーへのメッセージ表示、バックアップからファイル復元、ファイルのダウンロード、他のシステム・コマンドの実行、PC を再起動して同じオペレーティング・システムに入ったり、Rescue and Recovery ワークスペースに入ったりと切り替えたりすることが含まれます。リポジトリー機能とコマンドは両方とも、通常のオペレーティング・システム (Windows XP など) または Rescue and Recovery ワークスペースで働きます。

ウィルスに対抗する総合的な戦略は、悪意のあるコードの広がりと損害を低減し、パッチを当てて各 PC をクリーンアップしてから、復元された PC をネットワークに戻すことです。非常に破壊的で素早く広がるウィルスの場合、PC をネットワークから削除し、Rescue and Recovery ワークスペースですべての修復操作を行う必要があります。これが一番安全な方法ですが、通常の作業時間内にこの方法が取られる場合には、エンド・ユーザーにとっては破壊的でもあります。場合によっては、Rescue and Recovery ワークスペースへの移行のタイミングを遅らせたり、ネットワーク機能を制限することによって移行を回避したりできます。次のステップは、パッチやクリーンアップ用のコードをダウンロードし、クリーンアップ・コードを実行して、パッチのインストールの準備をすることです。一般に、パッチはオペレーティング・システムの稼働中にインストールされるようになっていますが、クリーンアップおよびその他の操作は Rescue and Recovery ワークスペースで行う方が適切です。修正処置が完了すると、PC は、Windows XP が動作し、ネットワーク設定が復元された状態で、通常の操作に復元することができます。

次の 2 つのセクションでは、リポジトリー操作およびコマンドについて詳細に説明します。次に、機能のインストールおよび設定が紹介されます。以下のセクションは、テスト、破壊的なウィルスへの対応、ワイヤレスまたは仮想プライベート・ネットワーク (VPN) によって接続された PC へのアドレッシング、および破壊度が軽い問題の修正のために PC をどのように使用するかといった一般的な作業の例を示します。

リポジトリー

リポジトリー機能は、各 PC で稼働し、管理者からの新しいメッセージがないか定期的に確認します。確認は、スケジュールされた時間間隔で、またはいくつかの注目するイベント (たとえば、ブート、中断または休止からの再開、新しいネットワーク・アダプターの検出、および新しい IP アドレスの割り当て) が発生したときに行われます。リポジトリー機能は、登録されたディレクトリー (Windows 共有ロケーション、 HTTP の URL、FTP の URL) にメッセージがないかを探します。複数のメッセージが見付かる場合は、それらを名前をソートした順で処理します。一度に 1 つのメッセージのみが処理されます。メッセージは一度のみ正常に処理されま

す。メッセージの処理が失敗すると、デフォルトでは、再び試行されることはありませんが、失敗時に再試行することを、メッセージ内に指定できます。

メッセージをリポジトリー機能によって処理されるフォルダー内に配置する前に、管理者がメッセージをパッケージしておく必要があります。パッケージを作成する場合、管理者はメッセージを構成するすべてのファイルをフォルダー (またはそのサブフォルダー) に配置します。ファイルのうち 1 つは、基本コマンド・スクリプトである “GO.RRS” という名前が付いている必要があります。管理者は、オプションでこのメッセージに署名キーを使用できますが、使用する場合、キーはすべてのターゲット・システムに使用可能である必要があります。リポジトリー機能は、パッケージの保全性をチェックし、署名が提供されているかどうかチェックし、GO.RRS を実行する前にすべてのファイルをローカル・フォルダーに展開します。

基本コマンド・スクリプト・ファイル (GO.RRS) は、Windows コマンド・ファイルの構文に従います。これには、正しい Windows コマンドおよび、次のセクションでリストするコマンドを含むことができます。また、Python コマンド・インタープリターが Rescue and Recovery ワークスペースの一部としてインストールされるので、Python スクリプトも GO.RRS スクリプトから呼び出すことができます。

スクリプトの実行の最後に、メッセージから展開されたファイルはすべて削除されるので、スクリプトの終了後にファイルが必要な場合 (たとえば、再起動時のパッチのインストール) には、ファイルをメッセージ・フォルダーから移動する必要があります。

各 PC は、メッセージを確認するリポジトリーに関する設定を持っています。IT 管理者が、多数の PC をグループに分割して、各グループに異なるリポジトリー (ネットワーク共有) を割り当てることが適切な場合があります。たとえば、PC はファイル・サーバーへの接近性によって地理的にグループ化することができるでしょう。あるいは、PC は組織別 (技術、営業、またはサポートなど) にグループ化することもできます。

Antidote Delivery Manager コマンドおよび使用可能な Windows コマンド

Antidote Delivery Manager システムは、PC の操作を容易にするためのいくつかのコマンドを提供します。メッセージを作成したり、設定値を調整したりするためのコマンドに加えて、ネットワークの制御、オペレーティング・システムの状態の決定および制御、システム・インベントリーからの XML ファイルの検査、エンド・ユーザーへのクライアント PC 上の Antidote Delivery Manager スクリプトの進行状況を通知するといったコマンドがあります。NETWK コマンドは、ネットワークを有効または無効にしたり、ネットワークを限定されたネットワーク・アドレスのグループ内に制限したりします。INRR コマンドは、Windows XP オペレーティング・システムが稼働中であるかどうか、あるいは PC が Rescue and Recovery ワークスペースにあるかどうかを判別するために使用できます。REBOOT コマンドは、PC をシャットダウンして、Windows XP または Rescue and Recovery を起動するよう指定するために使用できます。MSGBOX アプリケーションでは、ポップアップ・ボックスでメッセージを表示してエンド・ユーザーに通知を行うことができます。メ

ッセージ・ボックスはオプションで「OK」および「取消」ボタンを含むことができるので、メッセージはエンド・ユーザーからの入力に基づいて異なる動作を行うことができます。

一部の Microsoft コマンドは Antidote Delivery Manager にも使用できます。許可されるコマンドには、コマンド・シェルに内蔵のコマンドすべて (たとえば、DIR や CD) が含まれます。その他の有用なコマンド、たとえばレジストリーを変更するための REG.EXE やディスクの整合性を検査するための CHKDSK.EXE が使用可能です。

標準的な Antidote Delivery Manager の使用方法

Antidote Delivery Manager システムを使用して、多種多様なタスクを実行することができます。以下の例は、このシステムをどのように使用できるかを示しています。

- **単純なシステムのテスト - 通知の表示**

  このシステムの最も基本的な使用法は、エンド・ユーザーへ文章を 1 つ表示することです。このテストを実行したり、他のスクリプトをデプロイメントの前にテストするための最も簡単な方法は、このメッセージを、管理者の PC のローカル・フォルダーであるリポジトリーに配置することです。このように配置することで、他の PC に影響を与えずに、スクリプトを素早くテストできます。

- **スクリプトの準備およびパッケージ化**

  GO.RRS スクリプトを Antidote Delivery Manager をインストール済みのいずれかの PC 上で作成します。`MSGBOX /MSG "Hello World" /OK` という行を含むようにします。GO.RRS を含むフォルダーで APKGMSG コマンドを実行してメッセージを作成します。

- **スクリプトの実行**

  メッセージ・ファイルを PC のリポジトリー・フォルダーのいずれか 1 つに配置し、正しく動作するか監視します。メール・エージェントが次回実行されると、メッセージ・ボックスは「皆さんこんにちは (Hello World)」テキストを表示します。このようなスクリプトは、ネットワーク・リポジトリーをテストしたり、中断モードから再開したときのリポジトリーのチェックなどの機能を明示したりするためにもよい方法です。

大規模なワームの攻撃

この例では、ウィルスに対抗するための考えられる 1 つのアプローチを明示します。基本的なアプローチは、ネットワークをオフにしてから、再起動して Rescue and Recovery に入り、修正ファイルを取得し、修復作業を実行してから、起動して Windows XP に戻り、パッチをインストールし、最後にネットワークを元に戻すことです。これらすべての機能は、フラグ・ファイルと RETRYONERROR コマンドを使用して、1 つのメッセージを用いて実行することができます。

1. **ロックダウン・フェーズ**

   最初に行う必要があることは、エンド・ユーザーにこれから何が起こるか通知することです。攻撃がそれほど重大でない場合には、管理者はエンド・ユーザーに

修正を先に延ばすという選択肢を与えることができます。最も保守的なケースでは、このフェーズは、ネットワーキングを無効にし、エンド・ユーザーが処理中の作業を保存するよう 15 分間などの短い時間を与えるために使用することもできます。RETRYONERROR を使用して、スクリプトを実行中にしたまま、PC を再起動して Rescue and Recovery ワークスペースに入ることができます。

2. **コード配信フェーズおよび修復フェーズ**

   ネットワークを無効にし、再起動して Rescue and Recovery ワークスペースに入ることにより感染の恐れは取り除かれたので、追加のコードを取得して、修復作業を行うことができます。ネットワークを有効にするか、追加のファイルを取得するために特定のアドレスのみが必要な時間の間許可されるようにできます。Rescue and Recovery ワークスペースに入っている間に、ウィルス・ファイルを削除したり、レジストリーをクリーンアップすることができます。残念ながら、パッチは Windows XP が稼働中であると想定しているため、新しいソフトウェアまたはパッチをインストールすることはできません。ネットワークが無効のまま、ウィルス・コードがすべて削除された状態で、再起動して Windows XP に入り、修復を完了するのが安全です。このときに書き込まれたタグ・ファイルは、再起動後にスクリプトをパッチ・セクションに誘導します。

3. **パッチおよびリカバリー・フェーズ**

   PC が再起動して Windows XP に入るとき、Antidote Delivery Manager は、エンド・ユーザーがログインする前に処理を再開します。パッチはこの時点でインストールする必要があります。新しくインストールしたパッチが PC を再起動するよう要求する場合は、これを最後として PC を再起動させることができます。すべてのクリーンアップとパッチが完了したら、ネットワークを有効にすることができ、エンド・ユーザーは、通常の操作が可能であるという通知を受けます。

小規模なアプリケーション更新

すべての管理業務が、先に説明したような徹底した対策を要求するわけではありません。パッチが入手可能であるが、ウィルスから攻撃を受けていない場合には、より緩やかなアプローチが適切なことがあります。

単一のスクリプトで、RETRYONERROR およびタグ・ファイルを使用して、操作を制御することができます。

1. **ダウンロード・フェーズ**

   このプロセスは、エンド・ユーザーにパッチがダウンロードされるが、後でインストールすればよいことを通知するメッセージ・ボックスで始まります。その次に、パッチをサーバーからコピーすることができます。

2. **パッチ・フェーズ**

   パッチ・コードをインストールする準備ができたので、エンド・ユーザーに警告して、インストールを開始するときが来ました。エンド・ユーザーが遅延を要求する場合は、遅延を追跡するためにタグ・ファイルを使用することもできます。おそらく後でパッチをインストールする要求は、より緊急性の高いものになるでしょう。Antidote Delivery Manager は、エンド・ユーザーが電源をオフにする

か、PC を再起動する場合でもこの状態を保持することに注意してください。エンド・ユーザーが許可を与えると、パッチがインストールされ、必要であれば、PC は再起動します。

VPN およびワイヤレス・セキュリティーの対応

Rescue and Recovery ワークスペースは、現在、リモート・アクセス Virtual Private Networks (VPN) やワイヤレス・ネットワーク接続をサポートしていません。PC が Windows XP でこれらのネットワーク接続のいずれかを使用しており、その後再起動して Rescue and Recovery に入る場合、ネットワークへの接続は失われます。したがって、Rescue and Recovery ではファイルおよび修正をダウンロードするためにネットワークが使用できないので、先の例にあったようなスクリプトは動作しません。

解決策は、必要なファイルをすべて元のメッセージにパッケージしておくか、再起動する前に必要なファイルをダウンロードすることです。これは、すべての必要なファイルを、GO.RRS のあるフォルダーに配置することによって行われます。スクリプト・ファイルは、必要なファイルをスクリプトが終了する (クライアント・システムで GO.RRS を含むディレクトリーが削除される) 前に、最終的な位置によく注意して移動する必要があります。パッチをメッセージ・ファイルの中に入れるのは、パッチが非常に大きい場合には、実用的でありません。この場合は、エンド・ユーザーに、ネットワークがパッチを含むサーバー以外に対して制限されることを通知する必要があります。そうすれば、パッチは、まだ Windows XP にいる間にダウンロードできます。これにより、Windows XP がウィルスにさらされる時間が延びるとはいえ、余分にかかる時間はおそらくそれほど長くありません。

第 8 章 ベスト・プラクティス

この章では、Rescue and Recovery、 Client Security Solution、および ThinkVantage 指紋認証ユーティリティーのベスト・プラクティスを示すシナリオを提示します。このシナリオでは、ハードディスク・ドライブの設定から始まり、何回かの更新を行い、デプロイメントまでの手順を説明しています。

Rescue and Recovery および Client Security Solution のインストールのデプロイメント例

ここでは、Rescue and Recovery と Client Security Solution を、 ThinkCentre PC と ThinkPad の両方にインストールする場合の例をいくつか挙げます。

ThinkCentre のデプロイメント例

これは、各製品を次のような仮定のカスタマー要件で ThinkCentre にインストールする場合の例です。

- **Administration**
  - Rescue and Recovery を使用して Sysprep の基本バックアップを作成
  - PC の管理にローカル管理者アカウントを使用
- **Rescue and Recovery**
  - Client Security のパスフレーズ (パスワード) を使用して Rescue and Recovery ワークスペースへのアクセスを保護
    - ユーザーはそれぞれのパスフレーズでログインする必要があり、それによって、各自の SafeGuard PrivateDisk ボリューム・ファイルを開いてファイルを救出することができます。
- **Client Security Solution**
  - エミュレーション・モードでのインストールおよび実行
    - Lenovo および IBM の PC は、すべてが TPM (セキュリティー・チップ) を備えているわけではありません。
  - Password Manager 非搭載
    - 代わりに企業向けシングル・サインオン・ソリューションを使用します。
  - Client Security パスフレーズを使用可能に設定
    - パスフレーズによって Client Security Solution アプリケーションを保護します。
  - Client Security Windows ログオンを使用可能に設定
    - Client Security パスフレーズで Windows にログインします。
  - すべてのユーザーに 500 MB の SafeGuard PrivateDisk を作成
    - 各ユーザーには、データを安全に保管するために 500 MB のスペースが必要です。
  - エンド・ユーザー・パスフレーズのリカバリー機能を使用可能に設定

- ユーザーが、自分で決めた 3 つの質問に答えることによって、パスフレーズをリカバリーできるようにします。
– Client Security Solution XML スクリプトをパスワード = “XMLscriptPW” で暗号化
  - パスワードによって、Client Security Solution 構成ファイルを保護します。

準備 PC で以下を実行します。

1. 「ローカル管理者」アカウントで Windows にログインします。
2. Rescue and Recovery および Client Security Solution プログラムを、次のオプションを指定してインストールします。

```
setup_tvtrnr3_1027.exe /s /v"/qn "EMULATIONMODE=1" "NOPWMANAGER=1"
"NOCSSWIZARD=1""
```

   注:

   a. tvt ファイル (z062zaa1025us00.tvt など) が実行可能ファイルと同じフォルダーにあることを確認します。同じフォルダーにない場合、インストールは失敗します。
   b. ダウンロードした実行可能ファイルの名前が setup_tvtrnr3_1027c.exe である場合、それは結合パッケージです。ここでの説明は、Large Enterprise の個々の言語ファイル・ダウンロード・ページから個別にダウンロードできるファイルを対象としています。
   c. 管理者インストールを実行する場合は、 133 ページの『今後発売される Lenovo および IBM ブランドの PC への Rescue and Recovery のインストール』を参照してください。
3. 再起動後はローカル管理者アカウントで Windows にログインし、デプロイメント用の XML スクリプトを作成します。コマンド・ラインから次のコマンドを実行してください。

```
"C:¥Program Files¥IBM ThinkVantage¥Client Security Solution¥css_wizarde.exe"
/name:C:¥ThinkCentre
```

   ウィザードで、次のオプションを選択します。

   - 「**拡張 (エキスパート・ユーザーのみ)**」→「**次へ**」を選択
   - 「**Client Security パスフレーズ (推奨)**」→「**次へ**」を選択
   - 「**Client Security ログイン画面を使用するログオン**」→「**次へ**」を選択
   - 管理者アカウント用の Windows パスワードを入力し、「**次へ**」を選択

     (たとえば WPW4Admin)
   - 管理者アカウント用の Client Security パスフレーズを入力し、「**Client Security パスフレーズを使用して、Rescue and Recovery ワークスペースへのアクセスを保護する**」ボックスにチェック・マークを付けて、「**次へ**」を選択

     (たとえば CSPP4Admin)
   - パスワードまたはパスフレーズの復元についての質問の選択画面が開きます。管理者アカウント用の 3 つの質問と回答を選択してから、「**次へ**」を選択
     a. 初めて飼ったペットの名前は?

        (たとえば Fluffy)

b. 好きな映画は?

(たとえば『風と共に去りぬ』)

c. 好きなスポーツ・チームは?

(たとえば Washington Redskins)

- 「**各ユーザーの暗号化 PrivateDisk ドライブを、選択された次の形式で作成します。**」のチェックを外し、「**次へ**」を選択
- 「要約」を確認し、「**適用**」を選択して xml ファイルを C:¥ThinkCentre.xml に書き込み、もう一度「**適用**」を選択
- 「**完了**」を選択してウィザードを閉じます。

4. テキスト・エディターで次のファイルを開き (XML スクリプト・エディターまたは Microsoft Word 2003 には XML フォーマット機能が組み込まれています)、以下の設定を変更します。
   - ドメイン設定への参照をすべて削除します。これにより、スクリプトには、各システムで代わりにローカル PC 名を使用するように通知されます。ファイルを保存します。
5. C:¥Program Files¥IBM ThinkVantage¥Client Security Solution¥xml_crypt_tool.exe のツールを使用して、XML スクリプトをパスワードで暗号化します。コマンド・プロンプトからファイルを実行します。構文は次のようになります。

   a. xml_crypt_tool.exe C:¥ThinkCentre.xml /encrypt XMLScriptPW

   b. これでファイルは C:¥ThinkCentre.xml.enc となり、パスワード = XMLScriptPW で保護されます。

これで、ファイル C:¥ThinkCentre.xml.enc をデプロイメント PC に追加する準備ができました。

デプロイメント PC で以下を実行します。

1. ローカル管理者アカウントで Windows にログインします。
2. Rescue and Recovery および Client Security Solution プログラムを、次のオプションを指定してインストールします。

```
setup_tvtrnr3_1027.exe /s /v"/qn "EMULATIONMODE=1" "NOPWMANAGER=1"
"NOCSSWIZARD=1""
```

   注:

   a. tvt ファイル (z062zaa1025us00.tvt など) が実行可能ファイルと同じフォルダーにあることを確認します。同じフォルダーにない場合、インストールは失敗します。

   b. ダウンロードした実行可能ファイルの名前が setup_tvtrnr3_1027c.exe である場合、それは結合パッケージです。ここでの説明は、Large Enterprise の個々の言語ファイル・ダウンロード・ページから個別にダウンロードできるファイルを対象としています。

   c. 管理者インストールを実行する場合は、133 ページの『今後発売される Lenovo および IBM ブランドの PC への Rescue and Recovery のインストール』を参照してください。

3. 再起動後、ローカル管理者アカウントで Windows にログインします。

4. 先に作成した ThinkCentre.xml.enc ファイルを、 C:¥ のルート・ディレクトリーに追加します。
5. レジストリーを変更して、全ユーザーでデフォルトの SafeGuard PrivateDisk Volume Size = 500 MB を設定します。これは、*reg* ファイルをインポートすると簡単にできます。
   a. HKEY_LOCAL_MACHINE¥SOFTWARE¥IBM ThinkVantage¥Client Security Software に移動します。
   b. 新規のストリング値 (値の名前: = PrivateDiskSize、値のデータ: = 500) を作成します。
   c. DWORD 値 (値の名前: = UsingPrivateDisk、値のデータ: = 1) を作成します。
6. RunOnceEx コマンドを、以下のパラメーターを指定して作成します。
   - RunonceEx キーに「0001」という新規キーを追加します。次のようになります。 HKEY_LOCAL_MACHINE ¥Software¥Microsoft¥Windows¥Current Version¥RunOnceEx¥0001
   - そのキーに、ストリング値の名前 「CSSEnroll」を次の値で追加します。 ″c:¥program files¥IBM ThinkVantage¥Client Security Solution¥vmservere.exe” C:¥ThinkCenter.xml.enc XMLscriptPW
7. “%rr%¥rrcmd.exe sysprepbackup location=L name=”Sysprep Backup” を実行します。システムの準備ができたら、次のように出力されます。

```
********************************************************
** Ready to take sysprep backup.                      **
**                                                    **
** PLEASE RUN SYSPREP NOW AND SHUT DOWN.              **
**                                                    **
** Next time the machine boots, it will boot          **
** to the PreDesktop Area and take a backup.          **
********************************************************
```

8. ここで Sysprep を実行します。
9. PC をシャットダウンしてから再起動します。 Rescue and Recovery ワークスペースで、バックアップ処理が開始されます。

   注: 注: 途中で復元と表示されますが、実際に行われているのはバックアップです。バックアップ後は、電源をオフにします。再起動はしないでください。

これで、Sysprep の基本バックアップが完了しました。

ThinkPad のデプロイメント例

これは、各製品を次のような仮定のカスタマー要件で ThinkPad にインストールする場合の例です。

- **Administration**
  – 既にイメージ化され、デプロイされているシステムにインストール
  – PC の管理にドメイン管理者のアカウントを使用
  – すべての PC に、BIOS スーパーバイザー・パスワード BIOSpw を割り当て
- **Client Security Solution**
  – TPM を活用
    - すべての PC にセキュリティー・チップを搭載

– Password Manager を使用可能に設定

– SafeGuard PrivateDisk を使用不可に設定

  - 代わりに、Utimaco SafeGuard Easy によるハードディスクの完全暗号化を活用します。

– Client Security Solution に対する認証として、ユーザーの Windows パスワードを活用

  - Utimaco SafeGuard Easy、Client Security Solution、および Windows ドメインに対する認証で、単一の Windows パスワードを許可

– Client Security Solution XML スクリプトを、パスワード = ″XMLscriptPW″ で暗号化

  - このパスワードによって、Client Security Solution 構成ファイルを保護します。

- **ThinkVantage 指紋認証ユーティリティー**

  – BIOS とハードディスクのパスワードを活用しない

  – 指紋によるログオン

    - 一定のセルフ・ユーザー登録期間後、ユーザーは、非管理者ユーザーの場合は指紋を必要とするセキュア・モード・ログオンに切り替えるため、デュアル・ファクター認証方式を効果的に実行できます。

  – 指紋チュートリアルの組み込み

    - エンド・ユーザーが、指紋を正しく読み取らせる方法や、操作を間違った場合は視覚的なフィードバックを得る方法を知ることができます。

準備 PC で以下を実行します。

1. 電源オフの状態から PC を始動し、**F1** を押して BIOS に入り、「Security」メニューに移動して「Clear Security Chip」を「Yes」にします。保管してから BIOS を終了します。
2. ドメイン管理者アカウントで Windows にログインします。
3. ThinkVantage 指紋認証ユーティリティーをインストールします。f001zpz2001us00.exe を実行して、Web パッケージから setup.exe ファイルを解凍します。setup.exe は、自動的に C:¥IBMTOOLS¥APPS¥TFS4.6-Build1153¥Application¥0409¥setup.exe に解凍されます。
4. f001zpz7001us00.exe を実行して Web パッケージから tutess.exe ファイルを解凍し、 ThinkVantage 指紋チュートリアルをインストールします。setup.exe は、自動的に C:¥IBMTOOLS¥APPS¥tutorial¥TFS4.6-Build1153¥Tutorial¥0409¥tutess.exe に解凍されます。
5. f001zpz5001us00.exe を実行して Web パッケージから fprconsole.exe ファイルを解凍し、 ThinkVantage 指紋コンソールをインストールします。f001zpz5001us00.exe を実行すると、setup.exe は、自動的に C:¥IBMTOOLS¥APPS¥fpr_con¥APPS¥UPEK¥FPR Console¥TFS4.6-Build1153¥Fprconsole¥fprconsole.exe に解凍されます。
6. Client Security Solution プログラムを、次のオプションを指定してインストールします。

```
setup_tvtcss6_1027.exe /s /v"/qn NOPRVDISK=1 NOCSSWIZARD=1 SUPERVISORPW=
"BIOSpw""
```

7. 再起動後はドメイン管理者のアカウントで Windows にログインし、デプロイメント用の XML スクリプトを作成します。コマンド・ラインから次のコマンドを実行してください。

```
"C:¥Program Files¥IBM ThinkVantage¥Client Security Solution¥css_wizard.exe"
/name:C:¥ThinkPad
```

ウィザードで、スクリプト例に合わせて次のオプションを選択します。

- 「拡張 (エキスパート・ユーザーのみ)」→「**次へ**」を選択
- 「Windows パスワード (簡易)」を選択し、「**次へ**」を選択
- 「指紋を使用するログオン」を選択し、「**次へ**」を選択
- ドメイン管理者アカウント用の Windows パスワードを入力し、「**次へ**」を選択

  (たとえば WPW4Admin)
- パスワードのリカバリーを有効にするためのチェックを外し、「**次へ**」を選択
- 要約を確認し、「適用」を選択して、 xml ファイルを C:¥ThinkPad.xml に書き込む
- 「**完了**」を選択してウィザードを閉じる

8. C:¥Program Files¥IBM ThinkVantage¥Client Security Solution¥xml_crypt_tool.exe のツールを使用して、XML スクリプトをパスワードで暗号化します。コマンド・プロンプトから、次の構文を実行します。
   a. xml_crypt_tool.exe C:¥ThinkPad.xml /encrypt XMLScriptPW
   b. これでファイルは C:¥ThinkPad.xml.enc となり、パスワード = XMLScriptPW で保護されます。

デプロイメント PC で以下を実行します。

1. 自社のソフトウェア配布ツールを使用して、ThinkVantage 指紋認証ユーティリティーの実行可能ファイル setup.exe (準備 PC から各デプロイメント PC に解凍されたもの) をデプロイします。setup.exe が PC に配信されたら、次のコマンドを実行してインストールを行います。

   ```
   setup.exe CTLCNTR=0 /q /i
   ```

2. 自社のソフトウェア配布ツールを使用して、ThinkVantage 指紋チュートリアルの実行可能ファイル tutess.exe (準備 PC から各デプロイメント PC に解凍されたもの) をデプロイします。tutess.exe が PC に配信されたら、次のコマンドを実行してインストールを行います。

   ```
   tutess.exe /q /i
   ```

3. 自社のソフトウェア配布ツールを使用して、ThinkVantage 指紋コンソールの実行可能ファイル fprconsole.exe (準備 PC から各デプロイメント PC に解凍されたもの) をデプロイします。
   - fprconsole.exe ファイルを「C:¥Program Files¥ThinkVantage 指紋認証ユーティリティー¥」フォルダーに入れます。
   - 次のコマンドを実行して、BIOS パワーオン・セキュリティー・サポートをオフにします。 fprconsole.exe settings TBX 0
4. 自社のソフトウェア配布ツールを使用して、ThinkVantage Client Solution 実行可能ファイル「setup_tvtcss6_1027.exe」をデプロイします。

- setup_tvtcss6_1027.exe が PC に配信されたら、次のコマンドを実行してインストールを行います。setup_tvtcss6_1027.exe /s /v"/qn NOPRVDISK=1 NOCSSWIZARD=1 SUPERVISORPW="BIOSpw""
- ソフトウェアをインストールすると、 TPM ハードウェアが自動的に使用可能になります。

5. システムの再起動後、次の手順で、 XML スクリプト・ファイルによるシステム構成を行います。
   - 先に作成した ThinkPad.xml.enc ファイルを、 C:¥ フォルダーにコピーします。
   - 以下を実行します。C:¥Program Files¥IBM ThinkVantage¥Client Security Solution¥vmserver.exe C:¥ThinkPad.xml.enc XMLScriptPW
6. 再起動後は、システムで Client Security Solution ユーザー登録の準備ができています。各ユーザーは、それぞれのユーザー ID と Windows パスワードでシステムにログインできます。システムにログインするすべてのユーザーに、Client Security Solution への登録を促すプロンプトが自動的に出され、登録すると、指紋読み取り装置への登録ができるようになります。
7. システムのすべてのユーザーが ThinkVantage 指紋認証ユーティリティーに登録されたら、セキュア・モード設定を使用可能にして、 Windows のすべての非管理者ユーザーに、各自の指紋でログオンさせるようにすることができます。
   - 次のコマンドを実行します。C:¥Program Files¥ThinkVantage 指紋認証ユーティリティー¥fprconsole.exe settings securemode 1
   - メッセージを削除するには、CTRL+ALT+DEL を押してパスワードでログオンします。ログオン画面で、次のコマンドを実行します。

     ```
     C:¥Program Files¥ThinkVantage 指紋認証ユーティリティー¥fprconsole.exe settings
     CAD 0
     ```

これで、Client Security Solution 6.0 と ThinkVantage 指紋認証ユーティリティーのデプロイメントが完了しました。

今後発売される Lenovo および IBM ブランドの PC への Rescue and Recovery のインストール

このセクションでは、Rescue and Recovery を使用した新規デプロイメントを説明します。

ハードディスク・ドライブの準備

システムをデプロイする際にまず最初にすべきことは、ドナー・システムのハードディスク・ドライブを準備することです。新規ハードディスクを使用してデプロイを行う場合、ハードディスクのマスター・ブート・レコードをきれいにする必要があります。

1. Windows をインストールするハードディスク以外のすべてのストレージ・デバイス (セカンド・ハードディスク、USB ハードディスク、USB メモリー・キー、PC カード・メモリーなど) はドナー・システムから取り外しておいてください。

重要: 以下のコマンドを実行すると、ターゲット・ハードディスク・ドライブの内容全体が消去されます。実行した後は、いかなるデータもターゲット・ハードディスク・ドライブからリカバリーすることができなくなります。

2. DOS 起動ディスケットを作成して、そのディスケットに CLEANDRV.EXE ファイルを入れます。
3. そのディスケットを起動します。DOS プロンプトで、次のコマンドを入力します。

```
CLEANDRV /HDD=0
```

4. ドナー・システムにオペレーティング・システムおよびアプリケーションをインストールします。ドナー・システムには、 Rescue and Recovery をインストールしないようにします。最後のステップで、Rescue and Recovery のインストールを行います。

インストール

最初に、InstallShield 形式の実行ファイル .EXE ファイルを C:¥RRTEMP フォルダーに解凍します。Rescue and Recovery を複数の PC にインストールする場合、このコマンドを 1 回行うことにより、各 PC のインストール時間が約半分に短縮されます。

1. インストール・ファイルが C ドライブのルートに置かれていることを前提として、ファイル EXE_EXTRACT.CMD を作成します。これは、ファイル C:¥SETUP_TVTRNR3_*XXXX*.EXE (ここで、 *XXXX* はビルド ID です) を C:¥RRTEMP フォルダーに解凍するスクリプト・ファイルです。

```
:: This package will extract the WWW EXE to the directory c:¥RRTemp for an
:: administrative install.
@ECHO OFF
:: This is the name of the EXE (Without the .EXE)
set BUILDID=setup_tvtrnr3_1027.exe
:: This is the drive letter for the Setu_tvtrnr3_1027.exe
:: NOTE: DO NOT END THE STRING WITH A "¥".  IT IS ASSUMED TO NOT BE THERE.
SET SOURCEDRIVE=C:
:: Create the RRTemp directory on the HDD for the exploded WWW EXMD c:¥RRTemp
:: Explode the WWW EXE to the directory c:¥RRTemp
:: Note: The TVT.TXT file must be copied into the same directory as the
:: MSI.EXE file.
start /WAIT %SOURCEDRIVE%¥%BUILDID%.exe /a /s /v"/qn TARGETDIR=c:¥RRTemp"
 TARGETDIR=c:¥RRTemp"
Copy Z062ZAA1025US00.TVT C:¥rrtemp¥
```

2. Rescue and Recovery のインストールの前に多くのカスタマイズを行うことができます。以下に、いくつかの例を示します。
   - 増分バックアップの最大数を 4 に変更する。
   - Rescue and Recovery が毎日午後 1:59 に「Scheduled」というラベル名で、ローカル・ハードディスクに増分バックアップを取るように設定する。
   - Rescue and Recovery ユーザー・インターフェースを、ローカル管理者グループに属していないすべてのユーザーから隠す。

3. TVT.TXT ファイルをカスタマイズします。一部のパラメーターは変更できます。詳しくは、 157 ページの『付録 B. TVT.TXT の設定および値』を参照してください。

```
[Scheduler]
Task1=RescueRecovery
Task2=egatherer
Task3=logmon

[egatherer]
ScheduleMode=0x04
Task=%TVT%¥Rescue and Recovery¥launcheg.exe
ScheduleHour=0
ScheduleMinute=0
ScheduleDayOfTheWeek=0
ScheduleWakeForBackup=0


[RescueRecovery]
LastBackupLocation=1
CustomPartitions=0
Exclude=0
Include=0
MaxNumberOfIncrementalBackups=5
EncryptUsingCSS=0
HideCSSEncrypt=0
UUIDMatchRequired=0
PasswordRequired=0
DisableSchedule=0
DisableRestore=0
DisableSFR=0
DisableViewBackups=0
DisableArchive=0
DisableExclude=0
DisableSingleStorage=0
DisableMigrate=0
DisableDelete=0
DisableAnalyze=0
DisableSysprep=1
CPUPriority=3
Yield=0
Ver=4.1
DisableBackupLocation=0
DeletedBackupLocation=0
HideLocationNotFoundMsg=0
HideMissedBackupMessage=0
HideNoBatteryMessage=0
SkipLockedFiles=0
DisableBootDisc=0
DisableVerifyDisc=0
HideAdminBackups=0
HideBaseFromDelete=0
HidePasswordProtect=0
HideSuspendCheck=1
HideBootUSBDialog=0
HideBootSecondDialog=1
HideNumBackupsDialog=1
HidePasswordPersistence=0
HideDiffFilesystems=0
PwPersistence=0
ParseEnvironmentVariables=1
MinAnalyzeFileSize=20
HideLockHardDisk=1
LockHardDisk=0
ResumePowerLossBackup=1
MinPercentFreeSpace=0
MaxBackupSizeEnforced=0
```

```
PreRejuvenate=
PreRejuvenateParameters=
PreRejuvenateShow=
PostRejuvenate=
PostRejuvenateParameters=
PostRejuvenateShow=
RunSMA=1
SPBackupLocation=0
ScheduleMode=4
ScheduleFrequency=2
ScheduleHour=12
ScheduleMinute=0
ScheduleDayOfTheMonth=0
ScheduleDayOfTheWeek=3
ScheduleWakeForBackup=0
Task=%TVT%¥Rescue and Recovery¥rrcmd.exe
TaskParameters=BACKUP location=L name="Scheduled" scheduled
SetPPArchiveBeforeBackup=1

[RestoreFilesFolders]
WinHiddenFolders=%RRBACKUPS%,%MININT%,%PREBOOT%,%HIBERFIL%,%PAGEFILE%,
%SYSVOLINFO%,%RECYCLER%
PEHiddenFolders=%RRBACKUPS%,%MININT%,%PREBOOT%,%HIBERFIL%,%PAGEFILE%,
%SYSVOLINFO%,%RECYCLER%,Z:¥
AllowDeleteC=FALSE

[logmon]
ScheduleMode=0x010
Task=%TVT%¥Common¥Logger¥logmon.exe
```

4. TVT.TXT ファイルと同じフォルダーに INSTALL.CMD ファイルを作成します。これは、以下のアクションを実行します。
   - TVT.TXT ファイルを C:¥RRTemp フォルダーに作成されたインストール・パッケージにコピーします。
   - インストール後に再起動を行わない Rescue and Recovery のサイレント・インストールを実行します。
   - Rescue and Recovery を起動して、基本バックアップを実行します。
   - サービスが開始されたら、Rescue and Recovery CD の ISO イメージを作成する環境をセットアップします (これは通常、再起動の一部として実行されます)。
   - ISO イメージを作成します。
   - 基本バックアップを作成し、PC を再起動します。
5. INSTALL.CMD コードを変更します。以下に INSTALL.CMD のコードを示します。

```
:: Copy custom TVT.txt here

copy tvt.txt "c:¥RRTemp¥Program Files¥IBM ThinkVantage¥Rescue and Recovery"

:: Install using the MSI with no reboot (Remove "REBOOT="R"" to force a reboot)

start /WAIT msiexec /i "c:¥TVTRR¥Rescue and Recovery - client security

 solution.msi" /qn REBOOT="R"

:: Start the service.  This is needed to create a base backup.

start /WAIT net start "Rescue and Recovery Service"

 :: Make an ISO file here - ISO will reside in c:¥Program Files¥IBM
ThinkVantage¥Rescue and Recoveery¥rrcd
```

注: Rescue and Recovery のインストール後に PC を再起動する場合、以下の環境変数の設定は不要です。

```
:: Set up the environment
```

```
set PATH=%PATH%;%SystemDrive%¥Program Files¥IBM ThinkVantage¥Common¥Python24

set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY

set TCL_LIBRARY=%SystemDrive%¥Program Files¥IBM ThinkVantage¥Common¥Python24
¥tcl¥tcl8.4

set TK_LIBRARY=%SystemDrive%¥Program Files¥IBM ThinkVantage¥Common¥Python24
¥tcl¥tk8.4

set PYTHONCASEOK=1

set RR=C:¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥

set PYTHONPATH=C:¥Program Files¥IBM ThinkVantage¥Common¥logger

:: The next line will create the ISO silently and not burn it

C:¥Program Files¥IBM ThinkVantage¥Common¥Python24¥python C:¥Program Files¥IBM
ThinkVantage¥Common¥spi¥mkspiim.pyc /scripted

:: Take the base backup... service must be started

c:

cd "C:¥Program Files¥IBM ThinkVantage¥Rescue and Recovery"

RRcmd.exe backup location=L name=Base level=0

:: Reboot the system

C:¥Program Files¥IBM ThinkVantage¥Common¥BMGR¥bmgr32.exe /R
```

カスタマイズ

ご使用の環境に Rescue and Recovery をデプロイしてあり、Rescue and Recovery で次の項目を変更する場合:

- 増分バックアップを 4 より大きく変更し、10 に変更する。
- バックアップの時刻に設定された午後 1:59 は、何らかの理由で環境に支障が生じたので、時刻を午前 10:24 に変更する。
- システム上のすべてのユーザーが、 Rescue and Recovery 3.0 のユーザー・インターフェースにアクセスできるようにする。
- 試験後の評価により、`Yield=` の値は標準値 `0` ではなく、`2` が適切であると判断し、スケジュール・バックアップの間、 PC をその他のプロセスに譲る。

これらの変更を複数の PC で行うには:

1. 次の内容を持つ UPDATE.MOD という mod ファイルを (テキスト・エディターを使用して) 作成します。

   ```
   [RescueRecovery] MaxNumberOfIncrementalBackups=10

   [rescuerecovery] ScheduleHour=10

   [rescuerecovery] ScheduleMinute=24

   [rescuerecovery] GUIGroup=

   [rescuerecovery] Yield=2
   ```
2. 次に、以下のように INSTALL.CMD ファイルを作成後、適当なシステム管理ツールを使用して、 INSTALL.CMD および UPDATE.MOD ファイルをターゲット・システムに配信します。各 PC 上で INSTALL.CMD を実行すると、更新が有効になります。以下に、INSTALL.CMD ファイルの内容を示します。

   ```
   :: Merge the changes into TVT.TXT

   "%RR%cfgmod.exe" "%RR%tvt.txt" update.mod

   :: Reset the scheduler to adopt the new scheduled backup time without a reboot

   "%RR%reloadsched.exe"
   ```

更新

Windows に Service Pack を適用するなど、PC に大規模な変更を加える必要があることがあります。Service Pack をインストールする前に、PC で増分バックアップを作成しておき、そのバックアップにラベルを付けることができます。以下のステップを実行します。

1. FORCE_BU.CMD ファイルを作成して、そのファイルをターゲット・システムに配信します。
2. FORCE_BU.CMD ファイルがターゲット・システムに置かれたら、それを起動します。

以下に FORCE_BU.CMD ファイルの内容を示します。

```
:: Force a backup now
"%RR%rrcmd" backup location=L name="Backup Before XP-SP2 Update"
```

Rescue and Recovery デスクトップの有効化

次に、Rescue and Recovery ワークスペースの利点を活用しましょう。説明のため、次のセクションでは、 Rescue and Recovery ワークスペースの制御ファイルを取得し、ユーザーが編集してから、RRUTIL.exe を使用して元の Rescue and Recovery ワークスペースに戻すことができるサンプルの UPDATE_RRE.CMD スクリプトを示します。IBMRRUTIL.EXE については、 23 ページの『RRUTIL.EXE の使用』を参照してください。

Predesktop Area を変更するため、UPDATE_RRE.CMD スクリプトはいくつかの手順を明示します。

- RRUTIL.exe を使用して、Rescue and Recovery ワークスペースからファイルを取得します。 Rescue and Recovery ワークスペースから取得するファイルは、ファイル GETLIST.TXT で定義されます。
- 適切なファイルを編集した後、ファイルを元の Rescue and Recovery ワークスペースを戻すためのフォルダー構造を作成しておきます。
- 保存して編集するために、ファイルのコピーを作成します。

この例では、エンド・ユーザーが Rescue and Recovery ワークスペースで「**ブラウザーを開く**」ボタンをクリックすると開かれるホーム・ページを変更します。 Web ページ `http://www.lenovo.com/thinkvantage` (英語のサイトです) が開きます。

変更を行うには、Notepad で PEACCESSIBMEN.INI ファイルを開いて、

1. 下記のように行を変更します。

```
button13 = 8, "Open browser", Internet.bmp, 1, 1, 0,
%sysdrive%¥Preboot¥Opera¥Opera.EXE, http://www.pc.ibm.com/cgi-
bin/access_IBM.cgi?version=4&link=gen_support&country=__
COUNTRY__&language=__LANGUAGE__
```

から次のように変更します。

```
button13 = 8, "Open browser", Internet.bmp, 1, 1, 0,
 %sysdrive%¥Preboot¥Opera¥Opera.EXE,
 http://www.ibm.com/thinkvantage
```

2. ファイルを Rescue and Recovery ワークスペースに配置するために用意したフォルダーにコピーします。詳しくは、 23 ページの『RRUTIL.EXE の使用』を参照してください。
3. PC を再起動して Rescue and Recovery ワークスペースに入ります。
4. PC 内のファイルについて、バックアップする必要があるファイルと、サーバー上にバックアップがあり、システム復元後に個別に復元できるため、バックアップしておく必要がないファイルを分析し、決定します。これを行うには、IBMFILTER.TXT ファイルを編集します。このファイルは NSF.CMD ファイルのあるフォルダーに置くことで、次の例に示すように、そこから正しい場所にコピーされます。

NSF.CMD:

```
copy ibmfilter.txt "%RR%"
```

IBMFILTER.TXT:

```
x=*.nsf
```

表 37. UPDATE_RR.CMD script

```
@ECHO OFF
::Obtain the PEAccessIBMen.ini file from the RR
c:¥RRDeployGuide¥RRUTIL¥RRUTIL -g getlist.txt
c:¥RRDeployGuide¥GuideExample¥RROriginal
:: Make a directory to put the edited file for import back into the RR
md c:¥RRDeployGuide¥GuideExample¥put¥preboot¥usrintfc
:: Open the file with notepad and edit it.
ECHO.
ECHO Edit the file
c:¥RRDeployGuide¥GuideExample¥RROriginal¥PEAccessIBMen.ini
```

File will open automatically

```
pause
:: Make a copy of original file
copy
c:¥RRDeployGuide¥GuideExample¥RROriginal¥preboot¥usrintfc¥PEAccessIBMen.ini
c:¥RRDeployGuide¥GuideExample¥RROriginal¥preboot¥usrintfc¥
PEAccessIBMen.original.ini
notepad
c:¥RRDeployGuide¥GuideExample¥RROriginal¥preboot¥usrintfc¥PEAccessIBMen.ini
pause
copy c:¥RRDeployGuide¥GuideExample¥RROriginal¥preboot¥usrintfc¥
PEAccessIBMen.ini c:¥RRDeployGuide¥GuideExample¥put¥preboot¥usrintfc
:: Place the updated version of the PEAccessIBMen into the RR
c:¥RRDeployGuide¥RRUTIL¥RRUTIL -p c:¥RRDeployGuide¥GuideExample¥put
ECHO.
ECHO Reboot to the RR to see the change
pause
c:¥Program Files¥IBM ThinkVantage¥Common¥BMGR¥bmgr32.exe /bw /r
```

GETLIST.TXT を以下の内容で作成します。

```
¥preboot¥usrintfc¥PEAccessIBMen.ini
```

Lenovo プリロードイメージ以外の PC への Rescue and Recovery のインストール

Rescue and Recovery をインストールするには、ハードディスク上のマスター・ブート・レコードで先頭の 8 セクターがブランクである必要があります。Rescue and Recovery は、リカバリー領域に入るためにカスタム・ブート・マネージャーを使用します。

マスター・ブート・レコードを使用する一部の他社製アプリケーションでは、製品のポインターがマスター・ブート・レコード・セクターに保存されます。このポインターが Rescue and Recovery のブート・マネージャーのインストールに干渉する場合があります。

下記のシナリオとベスト・プラクティスを参考にして、Rescue and Recovery により確実に望ましい機能と機能が提供されるようにしてください。

ハードディスク・ドライブのセットアップのベスト・プラクティス : シナリオ 1

このシナリオでは、Rescue and Recovery を含む新規イメージのデプロイメントを扱います。Rescue and Recovery を マスター・ブート・レコードを使用するアプリケーションがインストールされたクライアントにデプロイするには、下記のテストを行って、Rescue and Recovery に干渉するかどうかを判別します。

1. テスト・クライアントをセットアップする。
2. Rescue and Recovery をインストールします。マスター・ブート・レコードを使用する他のアプリケーションがあるために MBR の先頭 8 セクターに空きがない場合、次のエラー・メッセージが表示されます。

   ```
   Error 1722. There is a problem with this Windows
   Installer package. A program run as part of the
   setup did not finish as expected. Contact your
   personnel or package vendor.
   ```

基本オペレーティング・システムに OEM イメージを使用している場合、マスター・ブート・レコード に製品リカバリー・データが含まれていないことを確認してください。これは次の方法で行うことができます。

重要: 次のコマンドを実行すると、ターゲット・ハードディスク・ドライブの内容全体が消去されます。実行した後は、いかなるデータもターゲット・ハードディスク・ドライブからリカバリーすることができなくなります。

1. 以下の管理ツール・セクションから入手できる CLEANDRV.EXE ファイルを使用して、

   `http://www.lenovo.com/ThinkVantage`

   基本イメージの作成に使用するハードディスク・ドライブ上のマスター・ブート・レコードからすべてのセクターが消去されていることを確認する。
2. Windows をインストール後、ガイドに従ってイメージを作成する。

ハードディスク・ドライブのセットアップのベスト・プラクティス : シナリオ 2

Rescue and Recovery を既存のクライアントにデプロイするには、多少の努力と計画が必要です。

エラー 1722 を受け取り、8 つの空きセクターを作成する必要がある場合、Lenovo ヘルプ・デスクに連絡してエラーを報告し、さらなる指示を要請してください。

Rescue and Recovery の起動可能 CD (レスキュー・メディア) の作成

Rescue and Recovery ワークスペースを起動することができるレスキュー・メディア CD は、あらかじめ作成されている ISO イメージを展開するのではなく、現在のサービス領域の内容から作成します。ただし、適切な ISO イメージが以前に作成され、すでに存在する場合は、新しい ISO イメージを作成するのではなく、その ISO イメージを CD に書き出します。

ISO イメージの作成、CD への書き出しを行う場合、他のアプリケーションの起動を行わないようにしてください。これらの作業中に他のアプリケーションを実行すると、アプリケーションが強制終了することがあります。また、スクリーンセーバーや省電力設定も無効にしておくことを推奨いたします。
ハードディスク・ドライブの保護領域へのアクセスの性質上、管理者権限のあるユーザーのみが ISO イメージを作成することができます。ただし、制限ユーザーは ISO を CD に書き出すことは可能です。以下のファイルおよびフォルダーは、レスキュー・メディアに組み込まれます。

- minint
- preboot
- win51
- win51ip
- win51ip.sp1
- scrrec.ver

注: 新規 ISO イメージを作成する場合、上記のフォルダー・ファイルをコピーし、ISO をビルドするために、システム・ドライブに最低 400 MB の空き容量が必要です。この容量のデータを移動するのは HDD のスペックに依存するため、PC によっては 15 分以上かかる場合があります。

ISO ファイルの作成および CD への書き出しを行うサンプル・スクリプト: 次のコードを作成します。

```
:: Make an ISO file here - ISO will reside in c:¥IBMTOOLS¥rrcd
```

注: 以下の 7 行のコード (Bold フォントで表示) は、Rescue and Recovery のインストール後に再起動を行っていない場合にのみ必要です。

```
:: Set up the environment

set PATH=%PATH%;%SystemDrive%¥Program Files¥IBM ThinkVantage¥Common¥Python24

set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY

set TCL_LIBRARY=%SystemDrive%¥Program Files¥IBM ThinkVantage¥Common¥Python24
¥tcl¥tcl8.4
```

```
set TK_LIBRARY=%SystemDrive%¥Program Files¥IBM ThinkVantage¥Common¥Python24
¥tcl¥tk8.4

set PYTHONCASEOK=1

set RR=c:¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥

set PYTHONPATH=C:¥Program files¥IBM ThinkVantage¥Common¥logger

:: The next line will create the ISO silently and not burn it

c:¥Program Files¥IBM ThinkVantage¥Common¥Python24¥python c:¥Program Files¥
IBM ThinkVantage¥Common¥spi¥mkspiim.pyc /scripted

:: The next line will create the ISO with user interaction and not burn it

:: c:¥Program Files¥IBM ThinkVantage¥Common¥Python24¥python c:¥Program Files¥
IBM ThinkVantage¥Common¥spi¥mkspiim.pyc /scripted

/noburn
```

Rescue and Recovery のタイプ 12 のサービス区画へのインストール

Rescue and Recovery をタイプ 12 サービス区画にインストールするには、以下を用意する必要があります。

- SP.PQI ファイル。このファイルには、サービス区画を作成するための基本のブート可能ファイルが含まれています。
- PowerQuest PQDeploy
- Rescue and Recovery の最新インストーラ

Rescue and Recovery ワークスペースをサービス区画にインストールするには、いくつかの関連するオプションがあります。

注: タイプ 12 の区画は、 Windows と同じドライブ (C:¥ ドライブ) 上の区画テーブルで最後に使用された項目に置かれている必要があります。タイプ 12 の区画が HDD のどこにあるかは、 bmgr32 /info でわかります。詳しくは、 179 ページの『Rescue and Recovery ブート・マネージャーの設定 (BMGR32)』を参照してください。

インストールを行うには、以下の手順を実行してください。

1. ドライブの最後に最小 700 MB の未割り当ての空き容量を残しておきます。
2. PowerQuest を使用して、SP.PQI ファイルを未割り当ての空き容量に復元します。
3. ステップ 1 で作成した基本区画 (C ドライブを除く) を削除してから、再起動します。

   注: システム・ボリューム情報が新しく作成されたサービス区画に表示されます。システム・ボリューム情報は、Windows の「システムの復元」を「無効」に設定し、削除してください。
4. Rescue and Recovery をインストールし、再起動するようプロンプトが出たら、再起動します。

Sysprep のバックアップ/復元

パスワードの保存は、Sysprep のバックアップ/復元では機能しません。

Sysprep のバックアップが完了したら、電源をオフにし、システムを再起動してください。

Computrace と Rescue and Recovery

非 BIOS システムでは、Computrace のインストール後は、 Rescue and Recovery をアンインストールできません。

第 9 章 指紋認証ユーティリティー

指紋コンソールは 指紋認証ユーティリティー・インストール・フォルダーから実行する必要があります。基本的な構文は FPRCONSOLE [USER | SETTINGS] です。USER コマンドまたは SETTINGS コマンドは、どの操作セットを使用するかを指定します。たとえば、完全なコマンドは「fprconsole user add TestUser /FORCED」のようになります。コマンドがわからない場合やすべてのパラメーターが指定されていない場合は、短いコマンド・リストがパラメーターと共に表示されます。

指紋認証ユーティリティーおよび Management Console をダウンロードするには、次のリンクを使用してください。

http://www.lenovo.com/think/support/site.wss/document.do?sitestyle=lenovo&indocid=TVAN-EAPFPR (英語のサイトです。)

ユーザー固有コマンド

ユーザーの登録や編集を行う場合は、USER セクションを使用します。現行ユーザーが管理者権限を持っていない場合、コンソールの振る舞いは FS のセキュリティー・モードによって異なります。便利モード: 標準ユーザーでは、ADD、EDIT、および DELETE コマンドが使用できます。ただし、ユーザーは自分のパスポート (ユーザー名で登録) しか変更できません。セキュア・モード: どのコマンドも許可されません。構文は以下のとおりです。

`FPRCONSOLE USER` *`command`*

このとき、*command* は次のコマンドの 1 つです: ADD、EDIT、DELETE、LIST、IMPORT、EXPORT。

表 38.

コマンド	**構文**	**説明**	**例**
新規ユーザーの登録	`ADD [`*`username`*` [| `*`domain¥ username`*`]] [/FORCED]`	/FORCED フラグによってウィザードのキャンセル・ボタンは使用不可になるので、登録は必ず正常に終了する必要があります。ユーザー名が指定されない場合は、現行ユーザー名が使用されます。	`fprconsole add domain0¥testuser` `fprconsole add testuser` `fprconsole add testuser /FORCED`
登録ユーザーの編集	`EDIT [`*`username`*` [| `*`domain¥ username`*`]]`	ユーザー名が指定されない場合は、現行ユーザー名が使用されます。 **注:** 編集されるユーザーはまず自分の指紋を検査する必要があります。	`fprconsole edit domain0¥testuser` `fprconsole edit testuser`

表 38. (続き)

コマンド	構文	説明	例
ユーザーの削除	`DELETE [`*username* `[|` *domain¥ username* `| /ALL]]`	/ALL フラグは、この PC に登録されているすべてのユーザーを削除します。ユーザー名が指定されない場合は、現行ユーザー名が使用されます。	`fprconsole delete domain0¥testuser` `fprconsole delete testuser` `fprconsole delete /ALL`
登録ユーザーの列挙	`List`		
登録ユーザーのファイルへのエクスポート	`Syntax: EXPORT username [| domain¥username] file`	このコマンドは、登録ユーザーを HDD のファイルにエクスポートします。ユーザーは次に、別の PC 上、またはユーザーが削除されている場合は同じ PC 上の IMPORT コマンドを使用してインポートできます。	
登録ユーザーのインポート	`Syntax: IMPORT` *file*	IMPORT は指定したファイルからユーザーをインポートします。 **注:** ファイル上のユーザーが同じ指紋を使用してすでに同じ PC に登録されている場合は、識別操作でどちらのユーザーが優先順位を持つかは保証されません。	

グローバル設定のコマンド

指紋認証ユーティリティーのグローバル設定は、SETTINGS セクションによって変更できます。このセクションのすべてのコマンドには、管理者権限が必要です。構文は次のとおりです。

```
FPRCONSOLE SETTINGS command
```

このとき、*command* は次のコマンドの 1 つです: SECUREMODE、LOGON、CAD、TBX、SSO。

表 39.

コマンド	説明	構文	例
セキュリティー・モード	この設定は、指紋認証ユーティリティーの便利モードとセキュア・モードを切り替えます。	`SECUREMODE 0|1`	便利モードの設定は次のようにします。 `fprconsole settings securemode 0`

表 39. (続き)

コマンド	説明	構文	例
ログオン・タイプ	この設定は、ログオン・アプリケーションを使用可能 (1)、または使用不可 (0) にします。 /FUS パラメーターを使用する場合、PC の構成上可能であれば、ユーザーの簡易切り替えモードでログオンが可能です。	`LOGON 0|1 [/FUS]`	
CTRL+ALT+DEL メッセージ	この設定はログオンでの「CTRL+ALT+DEL を押す」テキストを使用可能 (1)、または使用不可 (0) にします。	`CAD 0|1`	
パワーオン・セキュリティー	この設定は、指紋認証ユーティリティーのパワーオン・セキュリティー・サポートをグローバルにオフ (0) にします。パワーオン・セキュリティー・サポートがオフになっている場合は、BIOS 設定に関係なく、パワーオン・セキュリティー・ウィザードやパワーオン・セキュリティー・ページは表示されません。	`TBX 0|1`	
パワーオン・セキュリティー・シングル・サインオン	この設定は、ユーザーが BIOS で検査された際に、自動的にユーザーをログオンさせるための logon で、BIOS で使用される指紋を使用可能 (1)、または使用不可 (0) にします。	`SSO 0|1`	

セキュア・モード対便利モード

ThinkVantage 指紋認証ユーティリティーは、便利モードとセキュア・モードの 2 つのセキュリティー・モードで実行することができます。

便利モードは高レベルのセキュリティーをそれほど重要視しない、ホーム PC を対象にしています。すべてのユーザーは、他のユーザーのパスポートの編集およびパスワードを使用して (指紋認証は行わない) システムにログオンするなどの、すべての操作を実行できます。

セキュア・モードは、より高レベルのセキュリティーが必要な状況を対象としています。特定の機能は管理者にのみ、予約されています。追加認証をせず、パスワードを使用してログオンできるのは管理者だけです。

管理者 は、ローカル管理者グループの任意のメンバーです。セキュア・モードを設定した後は、管理者だけが簡単モードに切り替えることができます。

セキュア・モード - 管理者

ログオンのとき、誤ったユーザー名やパスワードが入力された場合は、セキュア・モードでは次のメッセージが表示されます。「ユーザー名とパスワードでこの PC にログオンできるのは管理者だけです。」これは、セキュリティーを高め、ハッカーに対してログオンできない理由についての情報を与えるのを避けるために行われます。

表 40.

指紋	説明
新規パスポートの作成	管理者は自分のパスポートを作成することができ、また、制限ユーザーのパスポートも作成することができます。
パスポートの編集	管理者は自分のパスポートだけ を編集できます
パスポートの削除	管理者はすべての制限ユーザーとその他の管理者のパスポートを削除できます。他のユーザーがパワーオン・セキュリティーを使用している場合、管理者はパワーオン・セキュリティーからユーザー・テンプレートをオプションで削除することができます。
パワーオン・セキュリティー	管理者は、パワーオンで使用される制限ユーザーおよび管理者の指紋を削除することができます。 **注:** パワーオン・モードが使用可能な場合は、少なくとも 1 つの指紋がなければなりません。
設定	
ログオン設定	管理者はすべてのログオン設定を変更できます。
保護スクリーン・セーバー	管理者はアクセスできます
パスポート・タイプ	管理者はアクセスできます - サーバーと関連ある場合のみです。
セキュリティー・モード	管理者はセキュア・モードと便利モードを切り替えることができます。
Pro サーバー	管理者はアクセスできます - サーバーと関連ある場合のみです。

セキュア・モード - 制限ユーザー

Windows にログオン中は、制限ユーザーはログオンに指紋を使用する必要があります。指紋読み取り装置が作動していない場合は、管理者は指紋認証ユーティリティーの設定を便利モードに変更して、ユーザー名とパスワードによるアクセスを可能にする必要があります。

表 41.

指紋	
新規パスポートの作成	制限ユーザーはアクセスできません

表 41. (続き)

指紋	
パスポートの編集	制限ユーザーは自分のパスポートだけを編集できます。
パスポートの削除	制限ユーザーは自分のパスポートだけを削除できます。
パワーオン・セキュリティー	制限ユーザーはアクセスできません
設定	
ログオン設定	制限ユーザーはログオン設定を変更できません
保護スクリーン・セーバー	制限ユーザーはアクセスできます
パスポート・タイプ	制限ユーザーはアクセスできません
セキュリティー・モード	制限ユーザーはセキュリティー・モードを変更できません
Pro サーバー	制限ユーザーはアクセスできます - サーバーと関連ある場合のみです。

便利モード - 管理者

Windows へのログオン中は、管理者はユーザー名とパスワードを使用しても、指紋を使用してもログオンできます。 .

表 42.

指紋	
新規パスポートの作成	管理者は自分のパスポートだけ を作成できます。
パスポートの編集	管理者は自分のパスポートだけ を編集できます
パスポートの削除	管理者は自分のパスポートだけ を削除できます。
パワーオン・セキュリティー	管理者は、パワーオンで使用される制限ユーザーおよび管理者の指紋を削除することができます。 **注:** パワーオン・モードが使用可能な場合は、少なくとも 1 つの指紋がなければなりません。
設定	
ログオン設定	管理者はすべてのログオン設定を変更できます。
保護スクリーン・セーバー	管理者はアクセスできます
パスポート・タイプ	管理者はアクセスできます - サーバーと関連ある場合のみです
セキュリティー・モード	管理者はセキュア・モードと便利モードを切り替えることができます。
Pro サーバー	管理者はアクセスできます - サーバーと関連ある場合のみです。

便利モード - 制限ユーザー

Windows へのログオン中は、制限ユーザーはユーザー名とパスワードを使用しても、指紋を使用してもログオンできます。

表 43.

指紋	
新規パスポートの作成	制限ユーザーは自分のパスワードだけを作成できます。
パスポートの編集	制限ユーザーは自分のパスポートだけを編集できます。
パスポートの削除	制限ユーザーは自分のパスポートだけを削除できます。
パワーオン・セキュリティー	制限ユーザーは自分の指紋だけを削除できます。
設定	
ログオン設定	制限ユーザーはログオン設定を変更できません
保護スクリーン・セーバー	制限ユーザーはアクセスできます
パスポート・タイプ	制限ユーザーはアクセスできません - サーバーと関連ある場合のみです
セキュリティー・モード	制限ユーザーはセキュリティー・モードを変更できません
Pro サーバー	制限ユーザーはアクセスできます - サーバーと関連ある場合のみです。

ThinkVantage 指紋認証ユーティリティーおよび Novell Netware Client

ThinkVantage 指紋認証ユーティリティーおよび Novell のユーザー名とパスワードは一致する必要があります。

お使いの PC に ThinkVantage 指紋認証ユーティリティーがインストールしてあり、Novell Netware Client をインストールする場合は、レジストリーの一部の項目が上書きされることがあります。 ThinkVantage 指紋認証ユーティリティーのログオンで問題が発生した場合は、ログオン設定画面に移動して、ログオン・プロテクターを再度使用可能にしてください。

お使いの PC に Novell Netware Client がインストールされているが、インストール前に ThinkVantage 指紋認証ユーティリティーにログオンしていなかった場合、Novell のログオン画面が表示されます。画面で、必要な情報を入力してください。

ログオン・プロテクター設定を変更するには、次のようにします。

- 「コントロールセンター」を開始する。
- 「**設定**」をクリックする。
- 「**ログオン設定**」をクリックする。
- ログオン・プロテクターを使用可能または使用不可にする。

指紋ログオンを使用したい場合は、「Windows ログオン認証を通常のパスワード認証から指紋認証に置き換える」チェック・ボックスにチェック・マークをつけます。ログオン・プロテクターを使用可能、または使用不可にするには、再起動が必要なことに気をつけてください。

- お使いのシステムでユーザーの簡易切り替えがサポートされている場合は、これを使用可能または使用不可にする。
- (オプション機能) パワーオン・ブート・セキュリティーによって認証されたユーザーの自動ログオンを使用可能または使用不可にする。
- Novell ログオン設定を設定する。Novell ネットワークにログオンする場合は、次の設定が使用可能です。
  - **活動化**

    ThinkVantage 指紋認証ユーティリティーは自動的に既知の信用証明情報を提供します。 Novell のログオンが失敗すると、Novell Client ログオン画面が表示され、正しいデータの入力を要求するプロンプトが出されます。
  - **ログオン中の質問**

    ThinkVantage 指紋認証ユーティリティーは Novell Client ログオン画面を表示して、ログオン・データの入力を要求するプロンプトを出します。
  - **使用不可**

    ThinkVantage 指紋認証ユーティリティーは Novell ログオンを試行しません。

付録 A. インストール・コマンド・ライン・パラメーター

Microsoft Windows インストーラは、コマンド・ライン・パラメーターによって、複数の管理者機能を提供します。

管理用インストールの手順およびコマンド・ライン・パラメーター

Windows インストーラは、ワークグループによる使用またはカスタマイズのために、アプリケーションまたは製品のネットワークへの管理用インストールを実行できます。Rescue and Recovery インストール・パッケージの場合、管理用インストールによりインストール・ソース・ファイルが指定された場所に解凍されます。

- 管理用インストールを実行するには、セットアップ・パッケージをコマンド・ラインから /a パラメーターを使用して実行します。

```
Setup.exe /a
```

管理用インストールは、管理ユーザーにセットアップ・ファイルの解凍先を指定するようプロンプトを出すウィザードを表示します。デフォルトの解凍先の場所は C:¥ です。C: 以外のドライブ (その他のローカル・ドライブ、割り当てられたネットワーク・ドライブなど) の新しい場所を選択することもできます。新しいフォルダーも、この手順で作成できます。

- 管理用インストールをサイレント・インストールで実行する場合、解凍先の場所を指定するために、コマンド・ラインで次のように共通プロパティ TARGETDIR を設定することができます。

```
Setup.exe /s /v"/qn TARGETDIR=F:¥IBMRR"
```

または

```
msiexec.exe /i "Rescue and Recovery.msi" /qn TARGERDIR=F:¥IBMRR
```

管理用インストールを完了した後、管理者はソース・ファイルをカスタマイズ (たとえば、設定値を TVT.TXT に追加) することができます。

MSIEXEC.EXE の使用

TVT.TXT などカスタマイズした後に解凍したソースからインストールするには、ユーザーはコマンド・ラインで MSIEXEC.EXE を実行し、解凍された *.MSI ファイルの名前を引き渡します。MSIEXEC.EXE は、インストール・パッケージを解釈し、製品をターゲット PC にインストールするために使用するインストーラ プログラムです。

```
msiexec /i "C:¥WindowsFolder¥Profiles¥UserName¥
Personal¥MySetups¥project name¥product configuration¥release name¥
DiskImages¥Disk1¥product name.msi"
```

注: 上記のコマンドを、円記号の後にスペースを入れずに 1 行として入力します。

154 ページの表 44 は、MSIEXEC.EXE で有効なコマンド・ライン・パラメーターと、その使用方法を説明します。

表 44. コマンド・ライン・パラメーター

<table>
<tr><th>パラメーター</th><th>説明</th></tr>
<tr><td>/I package
または
product code</td><td>このフォーマットは製品のインストールに使用します。
<code>Othello:msiexec /i "C:¥WindowsFolder¥Profiles¥</code>
<code>UserName¥Personal¥MySetups</code>
<code>¥Othello¥Trial Version¥</code>
<code>Release¥DiskImages¥Disk1¥</code>
<code>Othello Beta.msi"</code>

製品コードとは、製品のプロジェクト・ビューの製品コード・プロパティで自動的に生成される GUID のことです。</td></tr>
<tr><td>/a package</td><td>/a オプションにより、管理者権限を持つユーザーは製品をネットワーク上にインストールできます。</td></tr>
<tr><td>/x package または product code</td><td>/x オプションは、製品をアンインストールします。</td></tr>
<tr><td>/L [i|w|e|a|r |u|c|m|p|v|+] log file</td><td>/L オプションを使用して作成すると、ログ・ファイルへのパスが指定されます。以下のフラグは、ログ・ファイルに記録する情報を示しています。
• i は、状況メッセージをログに記録します
• w は、致命的でない警告メッセージをログに記録します
• e は、すべてのエラー・メッセージをログに記録します
• a は、アクション・シーケンスの開始をログに記録します
• r は、アクション固有のレコードをログに記録します
• u は、ユーザー要求をログに記録します
• c は、初期ユーザー・インターフェース・パラメーターをログに記録します
• m は、メモリー不足メッセージをログに記録します
• p は、端末設定をログに記録します
• v は、冗長出力設定をログに記録します
• + は、既存ファイルに付加します
• * は、すべての情報を (冗長出力設定を除いて) ログに記録できるワイルドカード文字です</td></tr>
<tr><td>/q [n|b|r|f]</td><td>/q オプションを以下のフラグと併用して、ユーザー・インターフェース・レベルを設定します。
• q または qn は、ユーザー・インターフェースを作成しません。
• qb は、基本ユーザー・インターフェースを作成します。

下記のユーザー・インターフェース設定により、インストール終了時にモーダル・ダイアログ・ボックスが表示されます。
• qr は、縮小ユーザー・インターフェースを表示します。
• qf は、完全なユーザー・インターフェースを表示します。
• qn+ は、ユーザー・インターフェースを表示しません。
• qb+ は、基本ユーザー・インターフェースを表示します。</td></tr>
<tr><td>/? または /h</td><td>いずれかのコマンドにより、Windows インストーラの著作権情報が表示されます。</td></tr>
</table>

表 44. コマンド・ライン・パラメーター (続き)

パラメーター	説明
TRANSFORMS	**TRANSFORMS** コマンド・ライン・パラメーターを使用して、基本パッケージに適用する変換を指定します。変換のコマンド・ライン呼び出しは、以下のようになります。 `msiexec /i "C:¥`*`WindowsFolder`*`¥` `Profiles¥`*`UserName`*`¥Personal` `¥MySetups¥` `Your Project Name¥Trial Version¥` `My Release-1` `¥DiskImages¥Disk1¥` `ProductName.msi" TRANSFORMS="New Transform 1.mst"` 複数の変換をセミコロンで分離できます。そのため、Windows インストーラ・サービスが誤って解釈しないように、変換の名前にセミコロンを使用しないことをお勧めします。
Properties	すべての共通プロパティはコマンド・ラインで設定または変更できます。共通プロパティはすべて大文字であるため、専用プロパティと区別されます。たとえば、*COMPANYNAME* は共通プロパティです。 コマンド・ラインからプロパティを設定するには、次の構文を使用します。 `PROPERTY=VALUE` *COMPANYNAME* の値を変更するには、次のように入力します。 `msiexec /i "C:¥`*`WindowsFolder`*`¥` `Profiles¥`*`UserName`*`¥Personal` `¥` `MySetups¥`*`Your Project Name`*`¥` `Trial Version¥My Release-1` `¥` `DiskImages¥Disk1¥`*`ProductName.msi`*`"` *`COMPANYNAME`*`="InstallShield"`

付録 B. TVT.TXT の設定および値

以下のデフォルト値は、推奨設定値です。値は、プリロード・バージョン、Web ダウンロード・バージョンなどによって異なる場合があります。

表 45. TVT.TXT の設定および値

設定	**値**
AccessFile (GUIGroup を参照)	*filename*、このファイルは、Rescue and Recovery の操作を許可されている Windows ローカル・グループ (ドメイン・グループではない) の名前を含むファイルの完全修飾パスです。これが空白または欠落している場合、PC にログオンできるすべてのユーザーが GUI を起動し、コマンド・ライン操作を実行することができます。デフォルトでは、このファイルは空白です。
BackupPartition	バックアップを作成する区画の位置を指定します。 0 = 指定されたドライブの 1 次区画 1 = 指定されたドライブの 2 次区画 2 = 指定されたドライブの 3 次区画 3 = 指定されたドライブの 4 次区画 ドライブは、以下のセクションで指定します。 [BackupDisk] = ローカル・ハードディスク・ドライブ [SecondDisk] = セカンド・ローカル・ハードディスク・ドライブ [USBDisk] = USB ハードディスク・ドライブ **注:** 区画は事前に準備しておく必要があります。設定されていない場合、ユーザーに区画を設定するようプロンプトが出されます (宛先ドライブがユーザー・インターフェースで選択され、宛先ドライブに複数の区画がある場合) 。
BatteryPercentRequired	バックアップを作成するのに必要なバッテリーのパーセンテージです。AC 電源の時は適用されません。範囲は 0 から 100 です。デフォルトは 100 です。
CPUPriority	CPU の優先度を指定します。*n*、ここで *n* = 1 から 5 です。1 は最も低い優先度、5 は最も高い優先度です。 デフォルトは 3 です。
CustomPartitions -	0 = 各区画をバックアップ 1 = 各区画の IncludeInBackup を調べる
DisableAnalyze	0 = Optimize バックアップ・ストレージの optionEnable アーカイブを表示 1 = このオプションを隠す デフォルトは 0 です。

表 45. TVT.TXT の設定および値 (続き)

設定	値
DisableArchive	0 = アーカイブを有効にする 1 = アーカイブを無効にする デフォルトは 0 です。
DisableBackupLocation	0 = すべての宛先を有効にする 0x01 = ローカル宛先を無効にする 0x02 = CD/DVD ドライブを無効にする 0x08 = USB/ HDD を無効にする 0x10 = ネットワークを無効にする 0x20 = セカンド HDD を無効にする 1 = アーカイブを隠します これらを組み合わせて複数の場所をグレー表示にできます。たとえば、0x0A の値は CD/DVD および USB HDD を無効にし、0x38 の値は USB HDD、ネットワーク、およびセカンド HDD を無効にします。ローカル・ハードディスクのバックアップのみを有効にするには、0x3A の値 (または 0xFE) を指定します。
DisableBootDisc	0 = CD/DVD バックアップを作成するときに毎回、レスキュー・メディア (CD) を作成します 1 = 毎回、レスキュー・メディア (CD) を作成しない このオプションはバックアップ用のみ有効であり、アーカイブ用ではありません
DisableDelete	0 = バックアップの削除オプションを表示する 1 = このオプションを隠す デフォルトは 0 です。
DisableExclude	0 = ファイル/フォルダーの除外オプションを表示する 1 = ファイル/フォルダーの除外オプションを隠す デフォルトは 0 です。
DisableLiveUpdate	0 = LiveUpdate オプションを表示する 1 = このオプションを隠す デフォルトは 0 です。
DisableMigrate	0 = 「バックアップから移行ファイルを作成する」を表示する 1 = このオプションを隠す デフォルトは 0 です。

表 45. TVT.TXT の設定および値 (続き)

設定	値
DisableRestore	0 = システムの「復元」を有効にする 1 = システムの「復元」を隠す デフォルトは 0 です。
DisableSchedule	0 = スケジュールのバックアップ・オプションを表示する 1 = スケジュールのバックアップ・オプションを隠す デフォルトは 0 です。
DisableSFR	0 = 「ファイルの復元」を有効にする 1 = 「ファイルの復元」を隠す デフォルトは 0 です。
DisableSingleStorage	0 = 単一ストレージ・オプションを表示する 1 = このオプションを隠す デフォルトは 0 です。
DisableViewBackups	0 = バックアップの表示オプションを表示する 1 = このオプションを隠す デフォルトは 0 です。
DisableVerifyDisc	0 = 光学式書き込み操作を検査する 1 = 光学式書き込み操作を検査しない デフォルトは 0 です。
Exclude (Include を参照)	0 = GUIEXCLD.TXT を適用しない 1 = GUIEXCLD.TXT を適用する **注:** 1. 除外するファイルと包含するファイルは、インストール前に定義でき、インストール時に適用されます。 2. Exclude と Include の両方を 1 に設定することはできません。
GUIGroup (AccessFile を参照)	*group*、ここで *group* は Rescue and Recovery 操作が許可されている Windows ローカル・グループ (ドメイン・グループではない) です。特権グループのリストは、AccessFile 項目により定義されるファイルに格納されています。
HideAdminBackups	0 = リストに管理者バックアップを表示する 1 = 管理者バックアップを隠す デフォルトは 0 です。

表 45. TVT.TXT の設定および値 (続き)

設定	値
HideBaseFromDelete	0 = 「バックアップ削除」ダイアログで基本バックアップを表示する 1 = 「バックアップ削除」ダイアログで基本バックアップを隠す。 デフォルトは 0 です。
HideBootUSBDialog	0 = USB HDD へのバックアップでブートできない場合にプロンプトを表示する 1 = このプロンプトを隠す デフォルトは 0 です。
HideDiffFileSystems	0 = ファイルの復元/保管時に FAT/FAT32 区画を表示する 1 = ファイルの復元/保管時に FAT/FAT32 区画を隠す デフォルトは 0 です。
HideCSSEncrypt	0 = Client Security Solution を使用した暗号バックアップを隠さない 1 = Client Security Solution を使用した暗号バックアップを隠す デフォルトは 0 です。
HideGUI	0 = GUI を許可したユーザーにだけ表示する 1 = GUI を全ユーザーから隠す
HideLocationNotFoundMessage	バックアップ作成時、バックアップの保存先が見つからなかった場合のダイアログの表示有無を設定します。 0 = ダイアログ・メッセージを表示する 1 = ダイアログ・メッセージを隠す デフォルトは 0 です。
HideLockHardDisk	0 = MBR 破損からハードディスクを保護するオプションを表示する 1 = このオプションを隠す デフォルトは、1 です。
HideMissedBackupMessages	0 = ダイアログ・ボックスを表示する 1 = ダイアログ・ボックスを隠す デフォルトは、1 です。
HideNoBatteryMessage	バックアップの作成時、PC のバッテリーがない場合に表示されるダイアログの表示の有無について設定します。 0 = メッセージを表示する 1 = メッセージを隠す デフォルトは、1 です。

表 45. TVT.TXT の設定および値 (続き)

設定	値
HideNumBackupsDialog	0 = バックアップが最大数に達した時にユーザーにこれを示すダイアログを隠さない 1 = バックアップが最大数に達した時にユーザーにこれを示すダイアログを隠す デフォルトは、1 です。
HidePowerLossBackupMessage	0 = 電力損失をバックアップ・メッセージで表示する 1 = メッセージを隠す デフォルトは 0 です。
HidePasswordPersistence	「Rescue and Recovery パスワードの設定」ダイアログの表示に有無について設定します。 0 = GUI を隠す 1 = GUI を表示する デフォルトは 0 です。
HidePasswordProtect	バックアップ作成時に表示されるパスワードの保護について設定します。 0 = パスワード保護チェック・ボックスを表示する (デフォルト) 1 = パスワード保護チェック・ボックスを隠す デフォルトは 0 です。
HideSuspendCheck	0 = 「一時停止/休止状態から PC を起動する」チェック・ボックスを隠さない 1 = チェック・ボックスを隠す デフォルトは、1 です。
Include (Exclude を参照)	0 = GUIINCLD.TXT を適用しない 1 = GUIINCLD.TXT を適用し、包含するファイルおよびフォルダーを設定するためにオプションを表示する **注:** 1. 除外するファイルと包含するファイルは、インストール前に定義でき、インストール時に適用されます。 2. Exclude と Include の両方を 1 に設定することはできません。

表 45. TVT.TXT の設定および値 (続き)

設定	値
LocalBackup2Location	*x*¥*foldername*、ここで *x* = ドライブ名、および *foldername* は任意の完全修飾フォルダー名。 デフォルトは次のとおりです。 `1st partition letter on the second drive:¥IBMBackupData` **注:** 1. ドライブ名は変更される可能性があるため、Rescue and Recovery はインストール時にドライブ名を区画に関連付けて、ドライブ名ではなく区画情報を使用します。 2. これは、`TaskParameters` 項目が保存されている場所です。
LockHardDisk	0 = MBR を保護するためにハードディスクをロックしない 1 = ハードディスクをロックする デフォルトは 0 です。
MaxBackupSizeEnforced	*x*、ここで *x* は GB 単位のサイズです。この値により、バックアップがしきい値を超えないように防止されるわけではありません。ただし、しきい値を超えると、次回「要求時」バックアップを取る際に、ユーザーに対してファイル・サイズに関する警告が出されます。デフォルトは 0 です。
MaxNumberOf IncrementalBackups	増分バックアップの保存数 デフォルト = 5、最小 = 2、最大 = 32
MinAnalyzeFileSize *n*	ここで、*n* は「バックアップ・ストレージ・スペースの最適化」画面でユーザーに対してファイルを表示する際の、最小ファイル・サイズ (単位 MB) です。デフォルトは 20 です。
NetworkUNCPath	次のフォーマットを使用するネットワーク共有です。 `¥¥computername¥sharefolder` デフォルトはありません。 **注:** この場所は、フィルター・ドライバーにより保護されません。
NetworkUNCPath	*server share name*、たとえば ¥¥MYSERVER¥SHARE¥FOLDER
NumMinutes	*x*、ここでタスクは *x* 分経過後に実行される。
PasswordRequired	0 = Rescue and Recovery ワークスペースを開くためにパスワードを必要としない 1 = Rescue and Recovery ワークスペースを開くためにパスワードが必要
PDAPreRestore	*cmd*、ここで *cmd* は復元操作の前に Rescue and Recovery ワークスペースで実行するためのプログラムの完全修飾パスです。
PDAPreRestore *n*	*cmd*、ここで *cmd* は復元操作の前に Rescue and Recovery ワークスペースで実行するためのプログラムの完全修飾パスです。
PDAPreRestoreParameters	PDARestore プログラムで使用されるパラメーター。
PDAPreRestoreParameters *n*	PDARestore プログラムで使用されるパラメーター。
PDAPreRestoreShow	0 = タスクを隠す 1 = タスクを表示する

表 45. TVT.TXT の設定および値 (続き)

設定	値
PDAPreRestoreShow *n*	0 = タスクを隠す 1 = タスクを表示する
PDAPostRestore	*cmd*、ここで *cmd* は復元操作の前に Rescue and Recovery ワークスペースで実行するためのプログラムの完全修飾パスです。
PDAPostRestore *n*	*cmd*、ここで *cmd* は復元操作の前に Rescue and Recovery ワークスペースで実行するためのプログラムの完全修飾パスです。
PDAPostRestoreParameters	PDARestore プログラムで使用されるパラメーター。
PDAPostRestoreParameters *n*	PDARestore プログラムで使用されるパラメーター。
PDAPostRestoreShow	0 = タスクを隠す 1 = タスクを表示する
PDAPostRestoreShow *n*	0 = タスクを隠す 1 = タスクを表示する
Post (PostParameters を参照)	*cmd*、ここで *cmd* は基本タスクの後に実行される実行可能ファイルの完全修飾パスです。
Post (PostParameters を参照) *n*	ここで、*n* はバックアップ番号 0、1、2、3...32 です *cmd*、ここで *cmd* は基本タスクの後に実行される実行可能ファイルの完全修飾パスです。 例: • Post0=command.bat *path* これは基本バックアップ後に実行されます • Post1=command.bat *path* これは、増分バックアップ後に実行されます **注:** これはバックアップ専用です。
PostParameters (Post を参照)	*cmd*、ここで *cmd* は基本タスクの後に実行される実行可能ファイルの完全修飾パスです。これはバックアップ専用です。
PostParameters *n* (Post を参照)	`parms`、ここで *parms* は後タスクに使用されるパラメーターです。
	parms、ここで *parms* は後タスクに使用されるパラメーターです。 **注:** これはバックアップ専用です。
PostRestore	*cmd*、ここで *cmd* は復元操作の完了後に Windows で実行されるプログラムの完全修飾パスです。
PostRestore *n*	*cmd*、ここで *cmd* は復元操作の完了後に Windows で実行されるプログラムの完全修飾パスです。
PostRestoreParameters	PostRestore プログラムで使用されるパラメーター。
PostRestoreParameters *n*	PostRestore プログラムで使用されるパラメーター。
PostRestoreShow	0 = 復元タスクを隠す 1 = 復元タスクを表示する

表 45. TVT.TXT の設定および値 (続き)

設定	値
PostRestoreShow *n*	0 = 復元タスクを隠す 1 = 復元タスクを表示する
PostShow	0 = 後タスクを隠す 1 = 後タスクを表示する デフォルトは 0 です。
PostShow *n*	0 = 後タスクを隠す 1 = 後タスクを表示する デフォルトは 0 です。 ここで、*n* はバックアップ番号 0、1、2、3....32 です **注:** これはバックアップ専用です。
Pre (PreParameters を参照)	*cmd*、ここで *cmd* は基本タスクの前に実行される実行可能ファイルの完全修飾パスです。
Pre (PreParameters を参照) *n*	ここで、*n* はバックアップ番号 0、1、2、3....32 です *cmd*、ここで、*cmd* は基本タスクの前に実行される実行可能ファイルの完全修飾パスです。 例: • Pre0=command.bat *path* これは、基本バックアップ前に実行されます • Pre1=command.bat *path* これは、増分バックアップ前に実行されます **注:** これはバックアップ専用です。
PreParameters (Pre を参照)	ここで、*parms* は前タスクで使用されるパラメーターです
PreRejuvenate *cmd*	ここで、*cmd* は復元操作の前に Windows で実行されるプログラムの完全修飾パスです
PreRejuvenateParameters *parms*	ここで、*parms* は PreRejuvenate プログラムで使用されるパラメーターです。
PreRejuvenateShow	0 = タスクを隠す 1 = タスクを表示する
PostRejuvenate *cmd*	*cmd*、ここで、*cmd* は復元操作の後に Windows で実行されるプログラムの完全修飾パスです
PostRejuvenateParameters *parms*	ここで、*parms* は PostRejuvenate プログラムで使用されるパラメーターです。
PostRejuvenateShow	0 = タスクを隠す 1 = タスクを表示する

表 45. TVT.TXT の設定および値 (続き)

設定	値
PreShow	0 = 前タスクを隠す 1 = 前タスクを表示する デフォルトは、1 です。
PreShow *n*	ここで、*n* はバックアップ番号 0、1、2、3....32 です *cmd*、ここで、*cmd* は基本タスクの前に実行される実行可能ファイルの完全修飾パスです。 **注:** これはバックアップ専用です。
PreWinRestore	*cmd*、ここで *cmd* は復元操作の前に Windows で実行されるプログラムの完全修飾パスです。
PreWinRestore *n*	*cmd*、ここで *cmd* は復元操作の前に Windows で実行されるプログラムの完全修飾パスです。
PreWinRestoreParameters	PreWinRestore プログラムで使用されるパラメーター。
PreWinRestoreParameters *n*	PreWinRestore プログラムで使用されるパラメーター。
PreWinRestoreShow	0 = 後タスクを隠す 1 = 後タスクを表示する
PreWinRestoreShow *n*	0 = 後タスクを隠す 1 = 後タスクを表示する
ResumePowerLossBackup	0 = 最後のバックアップの途中で電力が遮断された場合にバックアップ処理を再開しない 1 = バックアップを再開する デフォルトは、1 です。
RunBaseBackup	0 = 基本バックアップを実行しない 1 = 基本バックアップを実行する デフォルトは 0 です。 `runbasebackuplocation=(Location)` 値は次のとおりです。 L = ローカル U = USB N = ネットワーク S = セカンド HDD C = CD

表 45. TVT.TXT の設定および値 (続き)

設定	値
ScheduleDayOfTheMonth	*x*、ここで *x* は 1 から 28 または毎月のバックアップのみ 35。(35 = 毎月の月末) 毎月のバックアップを選択した時に、何日にバックアップをするかを指定します。*x* = 1 〜 28 はその月の 1 日 〜 28 日を示します。また、35 を指定すると毎月の月末になります。
ScheduleDayOfTheWeek	毎週のバックアップを指定した時のみ有効 0 = 日曜日 1 = 月曜日 2 = 火曜日 3 = 水曜日 4 = 木曜日 5 = 金曜日 6 = 土曜日 デフォルトは 0 (日曜日) です。
ScheduleFrequency	0 = スケジュールを設定しない 1 = 毎日 2 = 毎週 3 = 毎月 デフォルトは 0 です。
ScheduleHour	*x*、ここで *x* は 0 から 23 で、0 は午前 12:00、12 は正午、23 は午後 11:00 PM です。 デフォルトは 0 です。
ScheduleMinute	*x*、ここで *x* は 0 から 59 で、増分バックアップを開始する時間の分を表します。 デフォルトは 0 です。
ScheduleWakeForBackup	0 = スケジュール・バックアップを行うために PC を復帰しない 1 = デスクトップのスケジュール・バックアップの場合は PC を復帰するが、ノートブック PC の場合は復帰しない 2 = デスクトップまたはノートブックに関わらず、PC を復帰する デフォルトは 2 です。 **注:** ノートブックがバックアップを行うために復帰しても AC 電源が接続されていなかった場合は、バックアップ操作が開始される前にスタンバイ/休止状態に戻ります。

表 45. TVT.TXT の設定および値 (続き)

設定	値
ScheduleMode	*x*、ここで *x* は次の値を持つビット・マスクです。 • 0 = スケジュールなし • 0x01 = 毎分 • 0x04 = 毎週 • 0x08 = 毎月 • 0x10 = サービスが開始されるたび (通常 PC の起動のたび) • 0x20 = PC が中断/休止から復帰する • 0x40 = USB HDD が接続された • 0x80 = ネットワークが接続された • 0x100 = ネットワークが切り離された • 0x200 = BIOS パスワード・リセット • 0x400 = マザーボード取り替え このパラメーターは、ユーザーが GUI の値を変更すると自動的に更新されます。ScheduleFrequency 値が TVT.TXT ファイルへの手動による変更またはスクリプト記述によって変更される場合、変更後 reloadsched を実行する必要があります。 **注:** ローカル・ハードディスクから USB HDD またはネットワークへのバックアップの自動同期の場合は、USB HDD が接続された または ネットワークが接続された のビットを設定する必要はありません。
SkipLockedFiles	0 = ロックされ、壊れたファイルが見つかった場合にダイアログ・ボックスを表示する 1 = ロックされ、壊れたファイルを常にスキップする
SPBackupLocation=2	サービス区画のバックアップを設定するために使用します。 この設定を使用しない場合、デフォルトの 500MB サービス区画は、ブート CD、復元 CD、およびサービス区画の他のデータが削除されるときに復元されます。
Task	*cmd*、ここで *cmd* は基本タスクとして実行されるプログラムの完全修飾パスです。 **注:** タスクの数は 50 を超えることはできません。
TaskParameter	*parms* は、タスクで使用されるパラメーターです。
TaskShow	0 = タスクを隠す 1 = タスクを表示する デフォルトは 0 です。
UUIDMatchRequired	0 = PC UUID の一致を必要としない (デフォルト) 1 = PC UUID の一致が必要 **注:** UUIDMatchRequired が 1 に設定される場合に取り込まれたバックアップには、この設定値が後で変更されても UUID の一致が必要です。

表 45. TVT.TXT の設定および値 (続き)

設定	値
Yield	*n*、ここで *n* は 0 から 8 です。0 は、Rescue and Recovery が他のコマンドに譲らないことを意味し、8 は Rescue and Recovery が最大限譲ることを意味します。 **注:** 他のコマンドに譲る値が高いほど、バックアップのパフォーマンスは徐々に遅くなります。 デフォルトは 0 です。

Rescue and Recovery のインストール後に、インストール・フォルダーにある TVT.TXT ファイルの設定を変更できます。設定は、インストール時には、デフォルト値が設定されています。

TVT.txt のバックアップおよび復元

サイレント・インストールをサポートするために、Rescue and Recovery のバックアップおよび復元の設定は、インストール前に編集された外部ファイル (*TVT.TXT*) によって定義されます。TVT.TXT ファイルは標準 Windows .ini ファイル・フォーマットに従い、データは [] によって示されるセクションおよび「設定=値」のフォーマットの行当たり 1 つの項目で設定されます。Rescue and Recovery はセクション・ヘッダー用に製品名を使用します (Rapid Restore Ultra など)。さらに、包含/除外フィルター・ファイルをインストール前に定義し、インストール時に適用することができます。

IT 管理者が設定値を使用してバックアップをカスタマイズする場合、インストール・フォルダーにある TVT.TXT ファイルを編集する必要があります。これを行うのに最も適したタイミングは、Rescue and Recovery をインストールする前、あるいはインストールした後最初のバックアップが行われる前です。TVT.TXT ファイルはすべてのバックアップ場所に保存されています。最初のバックアップ前、TVT.TXT ファイルは 1 つしかありません。バックアップ作成時に TVT.TXT を編集した場合、すべてのバックアップに変更されたファイルは同期されるので、TVT.TXT のバージョンの問題は発生しません。この場合、すべての TVT.TXT ファイルを最新の変更に更新する方法は 2 つあります。IT 管理者は、インストール・フォルダーの TVT.TXT ファイルをすべてのバックアップ・フォルダーにコピーするか、追加でバックアップを実行し、コマンドがすべての TVT.TXT バージョンをインストール・フォルダーのバージョンと同期させることです。望ましいのは、2 番目の方法です。

バックアップおよび関連タスクのスケジューリング

スケジューラーは Rescue and Recovery 固有に設計されていません。ただし、設定は同じ TVT.TXT ファイルに格納されます。Rescue and Recovery がインストールされると、スケジューラーは適切な設定値で取り込まれます。

以下に、スケジューラーの構造の説明を示します。
- 場所: インストール・フォルダー
- スケジュールを設定された各ジョブの項目
- 実行スクリプト

- 進行状況の通知に使用される名前付きパイプ。これはオプションです。
- スケジュール情報、つまり 毎月、毎週、毎日、平日、週末 (複数のスケジュール、たとえば、火曜日と金曜日は 2 つのスケジュールを作成することによりサポートされます)
- 関数に受け渡される変数

次の例を参考にしてください。Rescue and Recovery がスケジュールに従って増分バックアップを行い、バックアップの前後にコールバックを送る場合、下記の項目によりアプリケーションに適宜に命令が出されます。

```
[SCHEDULER]

Task1=rescuerecovery

[rescuerecovery]

Task="c:¥program
files¥ibm¥Rescue and Recovery¥

rrcmd.exebackup.bat"

TaskParameters=BACKUP
location=L name="Scheduled"

ScheduleFrequency=2

ScheduleDayOfTheMonth=31

ScheduleDayOfTheWeek=2

ScheduleHour=20

ScheduleMinute=0

ScheduleWakeForBackup=0

Pre="c:¥program files¥antivirus¥scan.exe"

Post="c:¥program files¥logger¥log.bat"
```

異なる TVT.txt ファイルの管理

ハードディスク・ドライブは複数の区画を持つことがあるので、バックアップおよび復元のプログラムは、バックアップ・データを格納するのはどの区画であるか知る必要があります。特定の宛先が複数の区画を持ち、バックアップ操作がスクリプトによって実行される場合、バックアップ操作の前に次の設定値を設定する必要があります。バックアップ操作をユーザーが手動で行う場合は、このセクションを無視することができます。

ローカル・ハードディスクへのバックアップの場合、設定値は TVT.TXT ファイルの BackupDisk セクションにあります。下記のように、セカンド・ローカル・ハードディスクへのバックアップは SecondDisk セクションを使用し、USB HDD へのバックアップは USBDisk セクションを使用します。

BackupPartition=*x*

ここで、*x* は 0 から 3 の範囲です。0 は該当するドライブの 1 つ目の区画を表します。

注: 区画は事前に準備しておく必要があります。設定されていない場合、GUI で選択された該当する宛先に複数の区画があるときは、ユーザーにプロンプトが出されます。たとえば、USB HDD の 2 つ目の区画にバックアップしたい場合は、TVT.TXT ファイルの項目は次のようになります。

```
[USBDisk]
BackupPartition=1
```

バックアップ用ネットワーク・ドライブの割り当て

ネットワーク・ドライブの割り当て機能は、MAPDRV.INI ファイルに依存します。このファイルは C:¥Program Files¥IBM ThinkVantage¥Common¥MND ディレクトリーにあります。すべての情報は、DriveInfo セクションに格納されます。

汎用命名規則 (UNC) 項目には、接続先の PC 名および共有が含まれます。

NetPath 項目は、mapdrv.exe からの出力される値です。これには、接続の作成時に使用された実際の名前が含まれます。

User および Pwd 項目は、ユーザー名およびパスワードの項目です。これらは暗号化されています。

以下に、ネットワーク・ドライブの割り当てを行うための項目の例を示します。

```
[DriveInfo]

UNC=¥¥server¥share

NetPath=¥¥9.88.77.66¥share

User=11622606415119207723014918505422010521006401209203708202015...

Pwd=11622606415100000000014918505422010521006401209203708202015...
```

デプロイメントの際、このファイルを同じユーザー名およびパスワードを使用する複数の PC で使用するようにコピーすることができます。UNC 項目は、Rescue and Recovery により TVT.TXT の値に従って上書きされます。

ネットワーク・バックアップ用のユーザー・アカウントのセットアップ

ネットワーク共有フォルダー上に RRBACKUPS フォルダーが作成されるとき、Rescue and Recovery のサービスにより、このフォルダーは読み取り専用フォルダーとして作成され、フォルダーを作成したアカウントのみ がフォルダーに対して完全な制御を持つようにアクセス権が割り当てられます。

マージ操作を完了するには、バックアップを作成しているユーザー・アカウントの変更許可が必要です。フォルダーを最初に作成したアカウント以外のアカウント (たとえば、管理者) でログインすると、マージ・コマンドは失敗してしまいます。これを回避するには、

1. 制限ユーザーでバックアップを取る。
2. ネットワークへのバックアップと同時にローカルへのバックアップも取る。

のどちらかを行うようにしてください。

付録 C. コマンド・ライン・ツール

企業の IT 管理者はコマンド・ライン・インターフェースを使用して、ローカルまたはリモートから ThinkVantage テクノロジーの機能を起動することもできます。設定情報は、リモートのテキスト・ファイル設定を介して保守することができます。

Antidote Delivery Manager

Mailman

これは、コマンド C:¥program files¥IBM ThinkVantage¥Rescue and Recovery¥ADM¥mailman.exe を使用します。このプログラムは、実行するタスクの Antidote リポジトリーを確認します。コマンド・ライン引数はありません。

Antidote ウィザード

このコマンド、AWizard.exe は、管理者がインストールした場所に配置されます。コマンド・ライン引数はありません。

パスワードの設定

パスワードについては、 39 ページの『パスワード』を参照してください。

CFGMOD

CFGMOD は、スクリプトを使用して TVT.TXT ファイルを更新する方法です。CFGMOD コマンドは、C:¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥ フォルダーにあります。バックアップ・スケジュールを変更する場合、このコマンドの後に RELOADSCHED を続けて実行する必要があります。このユーティリティーを実行するには、管理者権限が必要です。

構文:

```
cfgmod TVT.TXT mod file
```

MOD ファイルのフォーマットでは、1 つの項目ごとに 1 行が必要です。各項目には、セクション名 ([と] で区切られる)、パラメーター名、″=″、および値がこの順序で含まれます。たとえば、バックアップ・スケジュールを調整する場合、MOD ファイルの項目は次のようになります。

```
[rescuerecovery]ScheduleFrequency=1
[rescuerecovery]ScheduleHour=8
[rescuerecovery]ScheduleMinute=0
```

Client Security Solution

Client Security Solution には次のコマンド・ライン・ツールがあります。

SafeGuard PrivateDisk

コマンド・ライン・インターフェースは C:¥Program Files¥IBM ThinkVantage¥SafeGuard PrivateDisk¥ フォルダーにあります。構文は次のとおりです。

```
PDCMD
 [ADDCERT volumename /pw adminpassword /sn certSN [/acc access]]  |
 [LIST]  |
 [MOUNT volumename [/pw userpassword [/pt authmode]] [/ro]]  |
 [NEW volumename [/sz size] [/dl driveletter] [/fs filesystem]
   [/pw adminpassword] [/pwu userpassword]]  |
 [UNMOUNT volumename /f]  |
 [UNMOUNTALL [/f]]  |
 [SETPASSWORD volumename /pw adminpassword /pwu userpassword [/ro]]
```

パラメーターは表 46 に表示されます。

表 46.

パラメーター	**結果**
ADDCDERT	PrivateDisk ボリュームに証明書を追加します
LIST	このユーザーの PrivateDisk ボリュームをリストします
MOUNT	特定の PrivateDisk ボリュームをマウントします。
NEW	新規 PrivateDisk ボリュームを作成します
UNMOUNT	特定の PrivateDisk ボリュームをアンマウントします
UNMOUNTALL	すべての PrivateDisk ボリュームをアンマウントします
SETPASSWORD	PrivateDisk ボリュームにユーザー・パスワードを設定します
volumename	PrivateDisk ファイルを含むファイルの名前
pw	パスワード
sn	証明書のシリアル番号。
acc	追加する証明書のアクセス・タイプ。有効な値は次のとおりです。 • **adm** 管理者のアクセス • **uro** ユーザーの読み取り専用アクセス • **usr** ユーザーの書き込みアクセス (デフォルト)

表 46. (続き)

パラメーター	結果
pt	認証方式。有効な値は次のとおりです。 • **0** 管理者のアクセス (デフォルト) • **1** ユーザー・パスワード • **2** 証明書に基づくログインの PIN
ro	読み取り専用
sz	サイズ (単位 キロバイト
dl	PrivateDisk ボリュームのドライブ名 (デフォルト = 使用可能な次のドライブ名)
fs	ファイル・システム。デフォルト値は次のとおりです。 • FAT (デフォルト) • NTFS
pwu	ユーザー・パスワード
f	強制操作

Security Advisor

これを GUI から実行するには、「**スタート**」→「**すべてのプログラム**」→「**ThinkVantage**」→「**Client Security Solution**」とクリックします。「**拡張**」をクリックして、「**セキュリティー設定の監査**」を選択します。これにより、C:¥Program Files¥IBM ThinkVantage¥Common¥WST¥wst.exe がデフォルトでインストールされます。

パラメーターは次のとおりです。

表 47.

パラメーター	説明
HardwarePasswords	1 か 0 に設定できます。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
PowerOnPassword	PowerOn パスワードを使用可能にする値か、設定にフラグを立てる値を設定します。
HardDrivePassword	ハードディスクのパスワードを使用可能にする値か、設定にフラグを立てる値を設定します。
AdministratorPassword	管理者パスワードを使用可能にする値か、設定にフラグを立てる値を設定します。

表 47. (続き)

パラメーター	説明
WindowsUsersPasswords	1 か 0 に設定できます。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
パスワード	ユーザー・パスワードを使用可能にする値か、設定にフラグを立てる値を設定します。
PasswordAge	この PC 上での、Windows のパスワードの使用日数の値を設定するか、設定にフラグを立てる値を設定します。
PasswordNeverExpires	Windows のパスワードが期限切れにならない値を設定するか、設定にフラグを立てる値を設定します。
WindowsPasswordPolicy	1 か 0 に設定できます。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
MinimumPasswordLength	この PC 上でのパスワードの長さの値を設定するか、設定にフラグを立てる値を設定します。
MaximumPasswordAge	この PC 上でのパスワードの使用日数の値を設定するか、設定にフラグを立てる値を設定します。
ScreenSaver	1 か 0 に設定できます。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
ScreenSaverPasswordSet	スクリーン・セーバーにパスワードを要求する値を設定するか、設定にフラグを立てる値を設定します。
ScreenSaverTimeout	この PC 上でのスクリーン・セーバーのタイムアウトの値を設定するか、設定にフラグを立てる値を設定します。
FileSharing	1 か 0 に設定できます。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
AuthorizedAccessOnly	ファイル共用のための許可されたアクセスを設定する値を設定するか、設定にフラグを立てる値を設定します。
ClientSecurity	1 か 0 に設定できます。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
EmbeddedSecurityChip	セキュリティー・チップを使用可能にする値を設定するか、設定にフラグを立てる値を設定します。

表 47. (続き)

パラメーター	説明
ClientSecuritySolution	この PC 上で使用する CSS のバージョンの値を設定するか、設定にフラグを立てる値を設定します。

すべての値に対する別のオプションは無視されます。つまり、値は表示されますが、この値は比較には含まれません。 Security Advisor が稼動している場合は、1 つの HTML ファイルが c:¥ibmshare¥wst.html に書き込まれており、1 つの生データの XML ファイルが c:¥ibmshare¥wst.xml に書き込まれています。

例

[WST] セクションにはすべてのセクションが表示され、そのデフォルト値を設定するすべての設定があります。

```
[wst]
HardwarePasswords=1
PowerOnPassword=enabled
HardDrivePassword=enabled
AdministratorPassword=enabled

WindowsUsersPasswords=1
Password=enabled
PasswordAge=180
PasswordNeverExpires=false

WindowsPasswordPolicy=1
MinimumPasswordLength=6
MaximumPasswordAge=180

ScreenSaver=1
ScreenSaverPasswordSet=true
ScreenSaverTimeout=15

FileSharing=1
AuthorizedAccessOnly=true

ClientSecurity=1
EmbeddedSecurityChip=Enabled
ClientSecuritySolution=6.0.0.0
```

Security Advisor を隠したりカスタマイズするには、ファイル名 WST の TVT.txt ファイルにセクションを追加します。隠したりカスタマイズできる値は複数ありますが、TVT.txt ファイルに追加する必要があります。

Security Advisor を使用せず、GUI で使用可能であることを表示させたくない場合は、次の実行可能ファイルを削除します。

```
C:¥Program Files¥IBM ThinkVantage¥Common¥WST¥wst.exe
```

証明書転送ウィザード

証明書転送ウィザードを使用せず、GUI で使用可能であることを表示させたくない場合は、次の実行可能ファイルを削除します。

```
C:¥Program Files¥IBM ThinkVantage¥Client Security Solution
¥certificatetransferwizard.exe
```

Client Security ウィザード

このウィザードはハードウェアの所有権を取得し、ソフトウェアを構成し、ユーザーを登録するために使用します。 XML ファイルを介してデプロイメント・スクリプトを生成する際にも使用します。次のコマンドを実行して、ウィザードの機能を理解することができます。

```
C:¥Program Files¥IBM ThinkVantage¥Client Security Solution¥css_wizard.exe /?
```

表 48.

パラメーター	結果
/h または /?	ヘルプ・メッセージ・ボックスを表示します
/name:*FILENAME*	生成されたデプロイメント・ファイルの完全修飾パスおよびファイル名の前に付けます。このファイルには拡張子 .xml が付きます。
/encrypt	AES 暗号化を使用してスクリプト・ファイルを暗号化します。暗号化される場合、そのファイル名には .enc が付加されます。/pass コマンドを使用しない場合は、静的パスフレーズを使用して、ファイルを隠します。
/pass:	暗号化されたデプロイメント・ファイルを保護するために、パスフレーズの前に付けます。
/novalidate	ウィザードのパスワードとパスフレーズのチェック機能を使用不可にして、すでに構成済みの PC 上でスクリプト・ファイルを作成できるようにします。たとえば、現行 PC の管理者パスワードは、社内で要求される管理者パスワードではないことがあります。/novalidate コマンドを使用するとユーザーは xml ファイル作成中に css_wizard GUI に別の管理者パスワードを入力できます。

このコマンドの例を次に示します。

```
css_wizarde.exe /encrypt /pass:my secret /name:C:¥DeployScript /novalidate
```

注: システムがエミュレーション・モードで実行されている場合、実行可能ファイル名は css_wizard.exe です

デプロイメント・ファイルの暗号化/暗号化解除ツール

このツールは Client Security XML デプロイメント・ファイルの暗号化/暗号化解除に使用します。次のコマンドを実行して、ツールの機能を理解することができます。

```
C:¥Program Files¥IBM ThinkVantage¥Client Security Solution¥xml_crypt_tool.exe. /?
```

パラメーターは表 49 に表示されます。

表 49.

パラメーター	結果
/h または /?	ヘルプ・メッセージを表示します

表 49. (続き)

パラメーター	結果
FILENAME	.xml または .enc の拡張子を持つ、完全修飾パス名またはファイル名。
encrypt または decrypt	.xml ファイルには /encrypt、.enc ファイルには /decrypt を選択します
PASSPHRASE	ファイルを保護するためにパスフレーズを使用する場合に必要なオプション・パラメーター。

例:

```
xml_crypt_tool.exe "C:¥DeployScript.xml" /encrypt "my secret"
```

および

```
xml_crypt_tool.exe "C:¥DeployScript.xml.enc" /decrypt "my secret"
```

デプロイメント・ファイル処理ツール

ツール vmserver.exe は Client Security XML デプロイメント・スクリプトを処理します。次のコマンドを実行して、ウィザードの機能を理解することができます。

```
C:¥Program Files¥IBM ThinkVantage¥Client Security Solution¥vmserver.exe /?
```

表 50.

パラメーター	結果
FILENAME	FILENAME パラメーターにはファイル拡張子 xml または enc がなければなりません。
PASSPHRASE	PASSPHRASE パラメーターは、拡張子 enc を持つファイルの暗号化解除に使用します。

このコマンドの例を次に示します。

```
Vmservere.exe  C:¥DeployScript.xml.enc "my secret"
```

注: システムがエミュレーション・モードで実行されている場合、実行可能ファイル名は vmserver.exe です

TPMENABLE.EXE

TPMENABLE.EXE ファイルはセキュリティー・チップをオンにしたりオフにするために使用します。

表 51.

パラメーター	説明
/enable または /disable (セキュリティー・チップをオンにする、またはオフにする)	セキュリティー・チップをオンにしたりオフにしたりします。
/quiet	BIOS パスワードまたはエラーのプロンプトを隠します
sp:*password*	BIOS 管理者/スーパーバイザーのパスワードです。パスワードの前後に引用符を使用してはいけません。

サンプル・コマンド:

```
tpmenable.exe /enable /quiet /sp:My BiosPW
```

eGatherer

eGatherer コマンドは C:¥Program Files¥IBM ThinkVantage¥common¥egatherer¥egather2.exe にあります。

egathere2.exe は収集した情報を使用して EG2 出力を作成します。ホーム・フォルダーに保管する、ローカル XML 出力ファイルも作成できます。 EG2 ファイルは内部フォーマットであることに注意してください。

2 つの XML ファイルが作成されます。1 つはシステム情報用で、もう 1 つはデモグラフィック情報用です。 XML ファイルの名前は、メーカー、モデル・タイプおよびシリアル番号を組み合わせて作成されます。たとえば、IBM-2373Q1U-99MA4L7.XML、IBM-2373Q1U-99MA4L7.DEMOGRAPHICS.XML のようになります。

スキャナーは、次のコマンド・ライン構文を使用して、コマンド・ラインから実行できます。

egather2.exe [-help] [-batch] [-silent] [-nolimit] [-local] [-listprobes] [-probe probename *probename*]

- **-help**

  短いヘルプ・メッセージを表示します。
- **-batch**

  特記事項を表示しません。
- **-silent**

  操作中に何も表示しません
- **-nolimit**

  すべてのイベント・ログを収集します。デフォルトは直前の 500 エントリーです。
- **-local**

  ローカル XML ファイルを作成します。
- **-listprobes**

  使用可能なプローブをリストします。
- **-probe**

  指定したプローブを実行します。

MAPDRV

MAPDRV コマンドは、ネットワーク・ドライブを割り当てるためのユーザー・インターフェースを起動します。 MAPDRV.EXE コマンドは、C:¥Program Files¥IBM ThinkVantage¥Common¥MND フォルダーにあります。ネットワーク・ドライブの割り当てのインターフェースは、以下のパラメーターをサポートします。

構文:

```
mapdrv [switches]
```

パラメーターを指定せずにコマンドを入力するとアプリケーションが起動します。情報を手動で入力する必要があります。

すべてのパラメーターの戻りコードは次のとおりです。

- **0** = 成功
- **> 0** = 失敗

表 52. MAPDRV パラメーター

パラメーター	**結果**
/nodrive	ドライブ名を接続に割り当てずにネットワーク接続を作成する
/pwd	この共有上でのユーザーのパスワード。
/set	バックアップおよび復元で使用する共用、ユーザー、およびパスワードを設定します。戻りコードは次のとおりです。
/s	サイレント。接続できるかどうかに関わらずユーザーにプロンプトを出さない。
/timeout	タイムアウト値を設定します。
/unc	フォーム ¥¥server¥share の共用名
/user	この共用のユーザー名。

/SET コマンドを使用する場合は、次のセクションが TVT.TXT ファイルに追加されます。これを、/UNC/USER および PWD パラメーターを使用して、次の例で示します。

```
mapdrv /set /unc sharename /user username /pwd password
[mapdrv]
UNC=¥¥test¥test
User=1EE22597AE4D
PWD=04E22197B34D95943ED5A169A0407C5C
```

Rescue and Recovery ブート・マネージャーの設定 (BMGR32)

ブート・マネージャー・インターフェースのコマンド・ライン・インターフェースは BMGR32 です。これは、フォルダー C:¥Program Files¥IBM ThinkVantage¥Common¥BMGR にあります。下表に、BMGR32 のスイッチとその結果を示します。

表 53. BMGR32 のパラメーター

bmgr32	**結果**
/B0	区画 0 から起動する (区画テーブルの順序に基づく)

表 53. BMGR32 のパラメーター (続き)

bmgr32	結果
/B1	区画 1 から起動する
/B2	区画 2 から起動する
/B3	区画 3 から起動する
/BS	サービス区画から起動する
/BW	Rescue and Recovery の隠し区画から起動する
/BWIN	WINPE から起動するための要求をリセットする。これは、起動する前に呼び出す必要があります。
/CFG*file*	設定ファイル・パラメーターを適用する。設定ファイルに関する詳細については、 183 ページの『RRCMD コマンド・ライン・インターフェース』を参照してください。
/DS	MBR データ・セクターを戻す (0 ベース)
/D*n*	変更をディスク n に適用する。ここで n は 0 ベースです (デフォルト: 環境変数「SystemDrive」または、「SystemDrive」が見つからない場合は「C:¥」を含むディスク)。
/H0	区画 0 を隠す
/H1	区画 1 を隠す
/H2	区画 2 を隠す
/H3	区画 3 を隠す
/HS	サービス区画を隠す
/P12	区画タイプを 12 に設定してサービス区画を隠す
/INFO	HDD 情報を表示する (8 つのフリー・セクターを検査します)
/INFOP	HDD 情報を表示する (16 のフリー・セクターを検査します)
/M0	Rescue and Recovery ワークスペースはサービス区画にある
/M1	Rescue and Recovery ワークスペースは C:¥PARTITION にある (Windows と Rescue and Recovery ワークスペースのデュアル・ブート)
/M2	Rescue and Recovery ワークスペースは DOS のあるサービス区画にある (Rescue and Recovery ワークスペースと DOS のデュアル・ブート、Lenovo 製または IBM 製のプリロードのみ)
/OEM	IBM 製または Lenovo 製 PC ではない。これにより、POST の後に強制的に F11 (デフォルト) キーを押す 2 回目のチェックが行われます。これは、IBM の古い PC で必要になる場合があります。
/Patch*n*	MBR パッチ・プログラムがアクセスできる変数を設定するためにのみインストール・プログラムに使用されます。
Patchfile*filename*	MBR パッチをインストールするためにのみインストール・プログラムに使用されます
/PRTC	パッチ戻りコードを検索するために、インストール・プログラムのみに使用されます
/IBM	IBM 製または Lenovo 製 PC である

表 53. BMGR32 のパラメーター (続き)

bmgr32	結果
/Q	サイレント
/V	冗長
/R	PC を再起動する
/REFRESH	データ・セクターの区画テーブル・エントリーをリセットする
/TOC *tocvalue*	BIOS TOC ロケーションを設定する (8 バイトのデータを表す 16 文字)
/U0	区画 0 を表示する
/U1	区画 1 を表示する
/U2	区画 2 を表示する
/U3	区画 3 を表示する
/US	サービス区画を表示する
/F*mbr*	RRE マスター・ブート・レコード・プログラムをロードする
/U	RRE マスター・ブート・レコード・プログラムをアンロードする
/UF	MBR プログラムを強制インストールまたはアンインストールする
/?	コマンド・ライン・オプションをリストする

/info 属性で bmgr.exe を起動する場合は、次の情報がダンプされます。

- **追加 MBR**

  最初のセクター以外の、MBR を含むセクター番号。
- **データ**

  MBR によって使用されるデータ・セクターのセクター番号。
- **パッチ・インデックス**

  MBR を使用して適用される任意のパッチのセクター番号。
- **Checksum return**

  チェックサム・エラーがない場合はこれは 0 でなければなりません。
- **ブート区画**

  サービス区画の 1 をデフォルトとする区画テーブル・インデックス。
- **Alt 区画**

  存在する場合は、DOS ブート可能領域を示す区画テーブル・インデックス。
- **オリジナル MBR**

  PC のオリジナル MBR が保管されているセクター番号。
- **IBM フラグ**

データ・セクターの値 (IBM または Lenovo 製 PC の場合は 1、それ以外の場合は 0)

- **Boot Config**

  PC のレイアウトを説明する際に使用されるインストール・オプションを説明します。サービス区画が使用されたか、仮想区画が使用されたかを示します。

- **署名**

  データ・セクターおよび最初のセクターにある署名の値。「NP」が含まれていなければなりません

- **休止期間**

  これは、F11 メッセージが画面に表示される際の待ち時間の秒数 ¼ です。

- **スキャン・コード**

  サービス領域をブートする場合に使用するキー。 F11 キーの場合は 85 です。

- **RR**

  BMGR では使用しません。Rescue and Recovery で設定します。

- **Prev Active Part**

  サービス領域からブートされますが、この値は前のアクティブ区画の区画テーブル・インデックスを含みます。

- **ブート状態**

  PC の現在の状況を判別するために MBR によって使用されます。 0 - OS から通常どおりブートする、1 - サービス OS からブートする、2 - サービス OS から標準 OS に戻ってブートする。

- **Alt ブート・フラグ**

  代替 OS、たとえば DOS からブートする

- **前の区画タイプ**

  サービス領域からブートされる場合、この値はそこからブートする前にサービス区画が設定された区画タイプを含みます。

- **前の IBM MBR Index**

  インストーラが使用します。

- **Patch IN: OUT**

  パッチ・コードを使用する場合、このコードの入力値と出力値。

- **F11 Msg**

  正しい BIOS 呼び出しがサポートされていないことをユーザーに表示するメッセージ

RELOADSCHED

このコマンドは、TVT.TXT で定義されているスケジュール設定を再ロードします。TVT.TXT にスケジュールの変更を加える場合、変更をアクティブにするために、このコマンドを実行する必要があります。

サンプル・コマンド:

```
C:¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥reloadsched
```

RRCMD コマンド・ライン・インターフェース

基本の Rescue and Recovery コマンド・ライン・インターフェースは RRCMD です。このコマンドは C:¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥reloadsched.exe サブフォルダーにあります。下記を参照して、Rescue and Recovery のコマンド・ライン・インターフェースを使用してください。

構文:

RRcmd *command filter=filterfile location=c* [name=*abc* | level=*x*] [silent]

表 54. RRcmd パラメーター

コマンド	結果
Backup	通常のバックアップを行う (場所および名前のパラメーターを含める必要がある)
Restore	通常の復元を行う (場所とレベルを含める必要がある)
List	バックアップ・レベルに含まれるファイルをリストする (場所とレベルを含める必要がある)
Basebackup	代替基本バックアップを行う。これは増分バックアップの基礎として使用することができず、場所、名前、およびレベルを含める必要がある。レベルは 99 より大きくする必要がある。同じレベルを持つ別の基本バックアップがすでに存在する場合、それは上書きされる。

表 54. *RRcmd* パラメーター (続き)

コマンド	結果
`Sysprepbackup`	PC が再起動した後、Rescue and Recovery ワークスペースでバックアップ操作を行う。この機能の主な用途は、Sysprep のバックアップを取り込むことです。 **注:** 1. 場合によっては進行状況表示バーが移動しないことがあります。この場合、ハードディスクを listen してバックアップを行っているかどうかを確認することができます。バックアップが終了している場合は、バックアップが終了しているというメッセージを受け取ります。 2. ネットワークに対する sysprepbackup を作成するときにパスワードを指定すると、増分バックアップが行われるまでパスワード・ファイルはバックアップ・ロケーションに書き込まれません。以下に 2 つの回避方法を示します。 a. ローカル sysprep のバックアップを作成して、ネットワークか USB にバックアップをコピーする。 b. sysprep のバックアップ後にネットワークまたは USB に増分バックアップを作成し、その増分バックアップを維持するか削除する。
`Copy`	バックアップをある場所から別の場所にコピーする。これは、アーカイブとも呼ばれ、これには場所を含める必要がある。
`Rejuvenate`	指定したバックアップにオペレーティング・システムを復元する
`Delete`	バックアップを削除する。これには場所を含める必要がある。
`Changebase`	file.txt の内容に基づいて、すべてのバックアップ内のファイルを変更する。 file.txt 内のオプションは次のとおりです。 **A** 追加 **D** 削除 **RS** 置換
`migrate`	バックアップから移行ファイルを作成する
`filter=`*`filterfile`*	復元されるファイルおよびフォルダーを識別し、他のファイルを変更しない。これは、**restore** コマンドのみと併用されます。
`Location=`*`c`*	以下のいずれか 1 つ以上を選択することができる。 **L** は内蔵ハードディスク・ドライブ **U** は USB HDD **S** はセカンド・ハードディスク・ドライブ **N** はネットワーク **C** は CD/DVD 復元
`name=`*`abc`*	ここで *abc* はバックアップの名前

表 54. RRcmd パラメーター (続き)

コマンド	結果
`level=x`	ここで *x* は 0 (基本) から増分バックアップの最大数 (復元オプションでのみ使用される) までの数値。バックアップ・コマンドでは、 100 以上の level=*x* という数値は管理者バックアップでのみ必要とされます。 **注:** 1. 最新のバックアップから復元するには、このパラメーターを使用しないでください。 2. すべてのバックアップおよび復元は、適切な順序を維持したりコールバックを実行するなどのために、サービスを介して実行されます。サービスに送られるバックアップ・コマンドは、コマンド・ライン・オプションによって置換されます。
ブート・マネージャー設定ファイル・フォーマット	ブート・マネージャー設定ファイルのフォーマットは、以前のバージョンのブート・マネージャーと後方互換です。下記に示されていないスイッチはサポートされていません。ファイル・フォーマットはテキスト・ファイルで、各項目は別の行にあります。 `<PROMPT1=this is the text that will appear on F11 prompt>` `<KEY1=F11>` `<WAIT=40>`

System Migration Assistant

このモジュールは以前の SMA4.2 SMABAT.EXE と互換性があるコマンド・ライン・プログラムです。モジュールに対するコマンド・パラメーターおよび制御コマンドファイル (Commands.TXT) は SMA 4.2 と互換性がなければなりません。

Active Update

Active Update はローカル・システム上の更新クライアントを使用して、ユーザーとの対話を行わずに Web 上の希望するパッケージを配信します。 Active Update は使用可能な更新クライアントを照会し、使用可能な更新クライアントを使用して希望するパッケージをインストールします。 Active Update は ThinkVantage システム更新か、システム上のソフトウェア・インストーラを起動します。

Active Update のランチャーをインストールするかどうかを決定するには、次のレジストリー・キーの存在を確認します。HKLM¥Software¥Thinkvantage¥ActiveUpdate

Active Update を許可するように Active Update ランチャーを構成するかどうかを決定するには、HKLM¥Software¥IBMThinkvantage¥Rescue and Recovery は、EnableActiveUpdate 属性の値の独自のレジストリー・キーを検査する必要があります。 EnableActiveUpdate=1 は、Active Update のメニュー項目を、「ヘルプ」メニューの下に設定します。

Active Update

Active Update ランチャーをインストールするかどうかを決定するには、次のレジストリー・キーの存在を確認します。

```
HKLM¥Software¥TVT¥ActiveUpdate
```

Active Update を許可するように TVT.TXT ファイルを構成するかどうかを決定するには、TVT は EnableActiveUpdate 属性の値の独自のレジストリー・キーを検査する必要があります。 EnableActiveUpdate=1 の場合、TVT は「ヘルプ」メニューの下に「Active Update」メニュー項目を追加する必要があります。

Active Update を呼び出すには、呼び出し側 TVT が Active Update ランチャー・プログラムを起動して、パラメーター・ファイルを渡す必要があります (パラメーター・ファイルの説明については、「Active Update パラメーター・ファイル」を参照してください)。

Active Update を起動するには、次の手順に従います。

1. 1. Active Update ランチャーのレジストリー・キーを開く。

   ```
   HKLM¥Software¥TVT¥ActiveUpdate
   ```

2. 2. Path 属性の値を取得する。
3. 3. Program 属性の値を取得する。
4. 4. Path 属性と Program 属性で見つけた値を連結してコマンド・ストリングを形成する。
5. 5. パラメーター・ファイル (「Active Update パラメーター・ファイル」を参照) をコマンド・ストリングに追加する。
6. 6. コマンド・ストリングを実行する。作成されるコマンド・ストリングの例は、次のようになります。

   ```
   C:¥Program Files¥ThinkVantage¥ActiveUpdate¥activeupdate.exe C:¥Program
    Files¥ThinkVantage¥RnR¥tvtparms.xml
   ```

Active Update を起動する際の推奨される方法は非同期です。この場合、呼び出し側 TVT はブロックされません。呼び出し側 TVT が更新をインストールする前に終了する必要がある場合、インストール・プログラムが更新時に TVT を終了します。

Active Update パラメーター・ファイル

Active Update パラメーター・ファイルには、Active Update に渡される設定が含まれています。現在では、次の例で示すように TargetApp (TVT 名) のみが渡されます。

```
<root>
       <TargetApp>ACCESSIBM</TargetApp>
</root>
```

```
<root>
       <TargetApp>1EA5A8D5-7E33-11D2-B802-00104B21678D</TargetApp>
</root>
```

付録 D. 管理者ツール

ThinkVantage テクノロジーは、企業の IT 管理者向けのツールを提供します。

Antidote ウィザード

Antidote ウィザードについて詳しくは、193 ページの『付録 F. Antidote Delivery Manager コマンドの解説および例』を参照してください。

BMGR CLEAN

CleanMBR はマスター・ブート・レコードをクリーンアップします。このプログラムは、ブート・マネージャーのインストールに必要なセクターに十分な空きがないために Rescue and Recovery をインストールできないなどの、Rescue and Recovery インストール失敗が起こった場合に使用できます。

注:

1. このツールを実行すると、MBR を使用しているアプリケーションは使用できなくなります。たとえば、SafeGuard Easy、SafeBoot、および Computrace の MBR 版などがあります。
2. Rescue and Recovery をインストールする前にツールを実行する必要があります。
3. DOS の場合は cleanmbr.exe を使用し、Windows の場合は CleanMBR32.exe を使用できます。
4. DOS CleanMBR を実行した後で、FDISK /MBR を実行します。これは、MBR に置かれます。

CleanMBR32.exe のパラメーターは次のとおりです。

表 55.

パラメーター (必須)	**説明**
/A	MBR をクリアし、PC DOS MBR をインストールする
パラメーター (オプション)	
/Dn	ドライブへの変更を適用する。最初のドライブには *n*=0 を使用してください。
/Y	すべて Yes
/?	ヘルプを表示する
/H	ヘルプを表示する

CLEANDRV.EXE

すべてのファイルのドライブをクリーンアップする。このコマンドを実行した後には、オペレーティング・システムはありません。詳しくは、 142 ページの『Rescue and Recovery のタイプ 12 のサービス区画へのインストール』を参照してください。

CONVDATE

Convdate ユーティリティーは、Rescue and Recovery 管理ツールの一部として提供されます。このユーティリティーは日付と時間の 16 進値を決定し、日付と時刻の値を 16 進値に変換するのに使用し、またカスタム日付と時間を TVT.TXT のバックアップ・フィールドに設定するのに使用することができます。

```
[Backup0]
StartTimeLow=0xD5D53A20
StartTimeHigh=0x01C51F46
```

ユーティリティーを実行するには、次のようにします。

1. http://www.lenovo.com/thinkvantage (英語のサイトです) から Rescue and Recovery 管理ツールを抽出する。
2. CMD ウィンドウを開く
3. Convdate に入力する

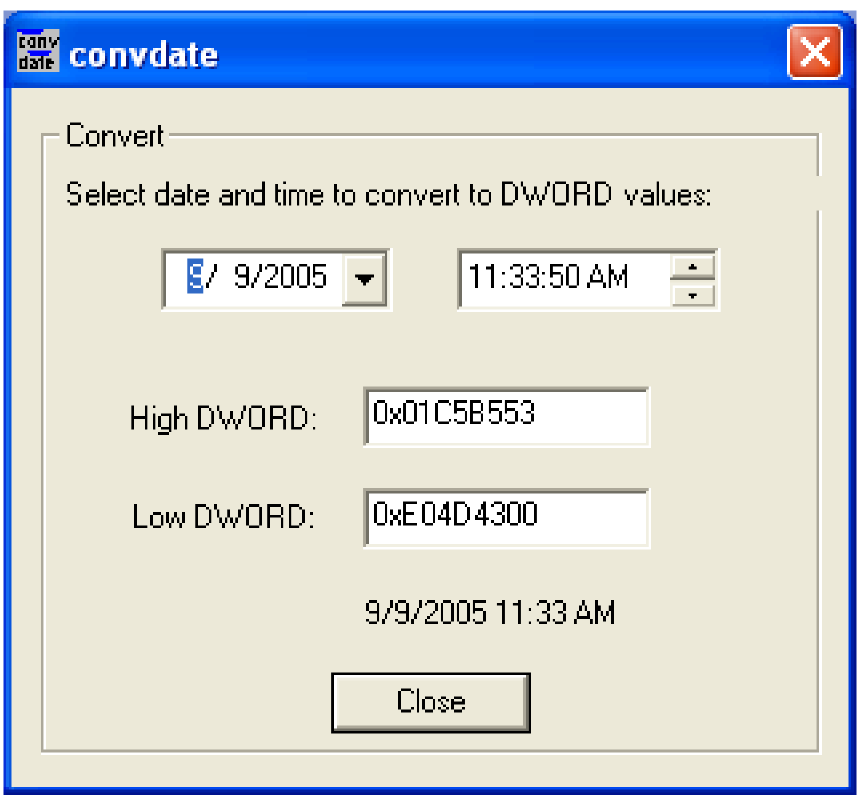


図 5. *Convdate ウィンドウ*

4. 「DWORD 値に変換する日付と時間を選択する」の下のフィールドの「日付と時間」に入力する。
5. 対応する TVT の .TXT ファイルの値は次のとおりです。
   - High DWORD=StartTimeHigh
   - Low Dword=StartTimeLow

CREAT SP™

このコマンドは、希望するメガバイトでサービス区画を作成します。ドライブ名はオプションです。

構文は次のとおりです。

```
createsp size=x drive=x /y
```

CREAT SP のパラメーターは次のとおりです。

表 56.

パラメーター	**説明**
size=*x*	作成するサービス区画のサイズ (メガバイト)
drive=*x*	サービス区画を作成するドライブのドライブ番号。指定しない場合は、最初の非 USB ドライブが使用されます。このパラメーターはオプションです。
/y	クリーンアップされるドライブの確認をしない。このパラメーターはオプションです。

注: bmgr32.exe は、createsp.exe と同じフォルダーにあり、WinPE から実行する必要があります。

RRUTIL.EXE

RRUTIL.EXE について詳しくは、 22 ページの『ワークスペース (Predesktop area)』を参照してください。

SP.PQI

このファイルはタイプ 12 のサービス区画の作成に使用できます。詳しくは、 142 ページの『Rescue and Recovery のタイプ 12 のサービス区画へのインストール』を参照してください。

付録 E. ユーザーの作業

ユーザー権限の種類によって実行できない機能があります。次の表に、制限ユーザー、パワー・ユーザー、および管理者ユーザー (OS がデフォルトで割り当てます) の基本的な操作機能の概要を示します。この機能は、Windows オペレーティング・システムによって若干、異なります。

Windows XP

次の表は、制限ユーザー、パワー・ユーザー、管理者ユーザーが Windows XP 環境の Rescue and Recovery で実行できる作業を示しています。

表 57. Windows XP のユーザー・タスク

Windows XP ユーザーが実行できる作業	**制限ユーザー**	**パワー・ユーザー**	**管理者**
レスキュー・メディア ISO を作成する	いいえ	いいえ	はい (後述のコマンド・ラインを使用して)
起動可能 CD メディアを作成する	はい	はい	はい
USB HDD 起動可能メディアを作成する	いいえ	いいえ	はい
バックアップを開始する	はい	はい	はい
Rescue and Recovery ワークスペース (RRE) で復元を開始する	はい	はい	はい
RRE で個別ファイルの復元を行う	いいえ (Windows) はい (Windows Pre Boot Area)	いいえ (Windows) はい (Windows Pre Boot Area)	はい
Rescue and Recovery インターフェースで包含および除外を設定する	はい	はい	はい
ネットワーク・ドライブにバックアップする	はい	はい	はい
バックアップのスケジュールを設定する	はい	はい	はい

Windows 2000

次の表は、制限ユーザー、パワー・ユーザー、管理者ユーザーが Windows 2000 環境の Rescue and Recovery で実行できる作業を示しています。

表 58. Windows 2000 のユーザー・タスク

Windows 2000 ユーザーが実行できる作業	制限ユーザー	パワー・ユーザー	管理者
レスキュー・メディア ISO を作成する	いいえ	いいえ	はい (後述のコマンド・ラインを使用して)
起動可能 CD メディアを作成する	はい	はい	はい
USB HDD 起動可能メディアを作成する	いいえ	いいえ	はい
バックアップを開始する	はい	はい	はい
Rescue and Recovery ワークスペース (RRE) で復元を開始する	はい	はい	はい
RRE で個別ファイルの復元を行う	いいえ (Windows) はい (Windows Pre Boot Area)	いいえ	はい
Rescue and Recovery インターフェースで包含および除外を設定する	はい	はい	はい
ネットワーク・ドライブにバックアップする	いいえ	いいえ	はい
バックアップのスケジュールを設定する	はい	はい	はい

レスキュー・メディアの作成

管理者は、次のコマンド・ラインを使用してレスキュー・メディア ISO を作成できます。このコマンドを実行すると、ISO ファイルを作成することができ、ファイルは自動的に C:¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥rrcd¥ フォルダーに置かれます。

```
:: This line will create the ISO silently and not burn it

C:¥Program Files¥IBM ThinkVantage¥Common¥Python24¥python" "C:¥Program Files¥IBM
  ThinkVantage¥Common¥spi¥mkspiim.pyc /scripted

 /scripted

:: This line will create the ISO with user interaction and not burn it

C:¥Program Files¥IBM ThinkVantage¥Common¥Python24¥python C:¥Program Files¥IBM
  ThinkVantage¥Common¥spi¥mkspiim.pyc /noburn

 /noburn
```

付録 F. Antidote Delivery Manager コマンドの解説および例

コマンド・ライン・パッケージ化ツールは、管理者がメッセージを作成できるようにします。また、Antidote Delivery Manager は、メッセージ内で使用される特殊なコマンド機能をいくつか提供します。

Antidote Delivery Manager コマンドのガイド

ブート・マネージャー・インターフェースのコマンド・ライン・インターフェースは BMGR32 です。これは、ディレクトリー C:¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥ADM にあります。下表に、BMGR32 のスイッチとその結果を示します。

表 59. Antidote Delivery Manager コマンド

コマンド	説明
APKGMES [/KEY *keyfile*|/NEWKEY *keyfile*|/NOSIG] *message_directory message_name*	APKGMES /KEY では、メッセージ・ファイルは *message_directory* の内容から作成されます。このフォルダーには GO.RRS という名前のファイルが含まれている必要があります。/KEY パラメーターが使用される場合、署名キーは keyfile.prv から取得され、keyfile.pub にあるキーは、メッセージを処理するすべてのクライアントに配布されていなければなりません。デフォルトでは、キー・ファイルには「KEYFILE.PRV」が使用されます。/NEWKEY パラメーターを使用してキーを作成することができます。署名が要求されない場合、/NOSIG を指定すると署名をしないことができます。メッセージ名の末尾に、*message_name*YYMMDDHHmm.zap のように日付スタンプが付加されます。
REBOOT [/*RR*|/Win] [/wait | /f]	このコマンドは PC を再起動します。パラメーターが指定されていない場合は、通常の起動シーケンスで再起動します。パラメーター RR は、再起動して Rescue and Recovery に入ることを意味し、WIN は再起動して通常のオペレーティング・システムに入ることを意味します。再起動はスクリプトを終了するまで発生しないので、これは通常スクリプト内の最後のコマンドであるはずです。オプションの WAIT コマンドは、PC に次回の再起動 (手動または他のメカニズムによって発生) 時に指定された環境に入るように強制します。/f パラメーターは、PC にすぐに再起動するよう強制し、開いているアプリケーションのデータをユーザーが保存するのを許可しません。パラメーターが指定されていない場合、プログラムはデフォルトで /win に入ります (/wait および /f が指定されていないものとみなします)。

表 59. Antidote Delivery Manager コマンド (続き)

コマンド	説明
`RETRYONERROR [ON│OFF] retries`	デフォルトで、スクリプトは 1 回のみ試行されます。ただし、スクリプトが正常に働くまでスクリプトを試行しつづけるのが重要な場合、RETRYONERROR コマンドを使用して、再試行パラメーターによって指定された有限の回数だけこのスクリプトの実行を試行し続けるよう通知することができます。回数が指定されない場合、デフォルト値は 3 です。グローバル・デフォルト値は、TVT.TXT ファイルのレスキュー・セクション `retries = retries` で設定できます。再試行は FOREVER に設定することもできますが、これによって無限ループが発生する恐れがあります。
`MSGBOX /msg message text [/head header_text] [/OK] [/CANCEL]│ [/TIMER timeout] /B3`	MSGBOX コマンドは、エンド・ユーザーがログオンされている場合は、このユーザーにメッセージを表示します。メッセージは表示されたままになり、タイムアウトが発生するか、「取消」ボタンが押されるか、「**OK**」ボタンが押される (/OK が指定されている場合) までスクリプトはブロックされます。/CANCEL が指定されていない場合、「取消」ボタンはパネル上に表示されず、キャンセルするのは非常に難しくなります。コマンドは次のコードを返します。 • 0 = OK が押された • 1 = CANCEL • 2 = タイマーが時間切れ メッセージにあるテキストは、改行およびタブを表すためにそれぞれ ¥n および ¥t を使用してフォーマット設定できます。
`NETWK [/D│/E│/A [/IP ip_address │ /DN domain_name] [/NM netmask]`	NETWK /D (無効) は、すべてのネットワーク・アダプターを無効にして、すべてのネットワーク・トラフィックを停止します。ネットワークは、NETWK /E (有効) コマンドが実行されるまで無効になります。NETWK /A は、ネットワークを IP アドレスに制限します。IP アドレスは /IP スイッチ (ドット「.」付き 10 進数) または /DN (DNS 名) によって指定されます。/NM スイッチはネットワーク・マスクを提供します。/NM が提供されていない場合は、/IP または /DN によって指定された単一 PC のみがアクセス可能になります。このコマンドの状態は再起動されても存続するので、ネットワークは明示的に有効にする必要があります。
`APUBKEY [/ADD│/DELETE] asn_1_encoded_public_key`	APUBKEY コマンドにより、管理者は各 PC の Antidote Delivery Manager メッセージの署名キーをリモートから管理することができます。各 PC には、複数のキーを格納できます。署名されたメッセージが処理される場合、成功するキーが見付かるまで各キーが試行されます。キーは個別に名前が付けられていないので、内容によって参照する必要があります。新規のキーは ADD パラメーターを使用して追加し、DELETE パラメーターを使用して削除することができます。TVT.TXT で指定されたキーが 1 つでもある場合は、未署名メッセージ (/NOSIG で作成されたメッセージ) は使用できなくなります。

表 59. Antidote Delivery Manager コマンド (続き)

コマンド	説明
AUNCPW [/Add|/CHANGE|/DELETE] *unc* [/USER *userid*] [/PWD *password*] [/REF *ref_name*]	このコマンドにより、ネットワーク・ドライブ用のパスワードを追加、変更、または削除することができます。UNC を使用する代わりに、参照名をメッセージ内のショートカットとして使用することができます。戻り値は次のとおりです。 • 0 = 成功 • 1 = 提供された情報を使用して設定できない • 2 = 成功、ただし同じ参照名を持つ別の UNC がすでに定義済み

表 59. *Antidote Delivery Manager コマンド (続き)*

コマンド	説明
`XMLtool for Conditionals`	条件付き (eGatherer、現在のハードウェア情報) • **使用法:** xmltool.exe *filename xpath function comparator value* – **filename** XML ファイルへのパスおよびファイル名 – **xpath** 値への完全修飾 xpath – **function** 次の値のいずれかである必要があります。 - /C、値を比較する (comparator および value も提供する必要がある) - /F、指定された値を %IBMSHARE%¥RET.TXT に書き込む – **Comparator:** 以下のいずれかである必要があります。 - LSS - LEQ - EQU - GTR - GEQ - NEW – **Value:** XML 項目がこの値と比較されます。 • 戻り値: – **0** 比較により真と評価されました (/c) – **1** 比較により偽と評価されました – **2** 誤ったコマンド・ライン・パラメーター – **3** XML ファイルを開く際のエラー (存在しないか、ファイルにエラーがある) – **4** 指定された XPATH が値を戻しません • **例:** `xmltool.exe %ibmshare%¥¥ibmegath.xml //system_summary/bios_version GEQ 1UET36WW`

表 59. Antidote Delivery Manager コマンド (続き)

コマンド	説明
`INRR`	INRR コマンドを使用してスクリプトが Rescue and Recovery ワークスペースで稼働中であるかどうか判別できます。戻り値は次のとおりです。 • 0 = 現行の OS が Win PE • 1 = 現行の OS が PE ではない • >1 = エラー
STATUS [/QUERY *location message_name* | /CLEAR *location*]	STATUS /QUERY コマンドを使用して、特定のメッセージがすでに実行されたか、実行されるのを待機しているか判別することができます。location の値は以下のいずれかである必要があります。 • **FAIL** メッセージがすでに実行され、失敗した • **SUCCESS** メッセージが正常に完了した • **WORK** メッセージが現在実行中か、Antidote Delivery Manager が次に実行されるときに実行される。 • **CACHE** メッセージが実行されるのを待機している。 STATUS/CLEAR コマンドは、指定された *location* をクリアします。戻り値は次のとおりです。 • 0 = 指定されたメッセージが検索されたか、コマンドが正常に完了した • 1 = 指定されたメッセージが検索されなかったか、コマンドが失敗した

サポートされる Microsoft コマンド

表 60. サポートされる Microsoft コマンド

コマンド	説明
ATTRIB.EXE	ファイル属性を表示または変更する
CACLS.EXE	ファイルのアクセス制御リスト (ACL) を表示または変更する
CHKDSK.EXE	ディスクを検査し、状況報告を表示する
COMP.EXE	2 つのファイルまたはファイルの集合の内容を比較する
COMPACT.EXE	NTFS 区画上のファイルの圧縮を表示または変更する
CONVERT.EXE	FAT ボリュームを NTFS に変換する。カレント・ドライブを変換することはできません。
DISKPART.EXE	ドライブを区画化する
FC.EXE	2 つのファイルまたはファイルの集合を比較し、それらの間の相違点を表示する
FIND.EXE	ファイル内のテキスト文字列を検索する

表 60. サポートされる Microsoft コマンド (続き)

コマンド	説明
FINDSTR.EXE	ファイル内の文字列を検索する
FORMAT.COM	ディスクを Windows で使用するようにフォーマット設定する
LABEL.EXE	変更を作成するか、ディスクのボリューム・ラベルを削除する
NET.EXE	ネットワーク・コマンドを指定する
PING.EXE	ネットワーク・リソースに到達できるか検査する
RECOVER.EXE	不良または欠陥のあるディスクから読み出すことのできる情報を復元する
REG.EXE	レジストリーの操作
REPLACE.EXE	ファイルを置換する
RRCMD.EXE	OS からバックアップを取るか、OS または RR ソート入力から復元を行うために使用する
SORT.EXE	入力をソートする
SUBST.EXE	パスをドライブ名と関連付ける
XCOPY.EXE	ファイルおよびフォルダー・ツリーをコピーする

準備およびインストール

準備

署名キーが使用される場合、管理者は新規の署名キーを生成するため、 /NEWKEY パラメーターを使用してパッケージ化ツールを実行する必要があります。

設定

いくつかの設定項目が必要となります。項目は TVT.TXT ファイルにあります。

リポジトリー

各クライアントはリポジトリーのリストを必要とします。これはフロッピーおよび C:¥、あるいは UNC で指定された少なくとも 1 つのネットワーク・ドライブです。`mailbox =` メールボックスの場所へのドライブおよびパス を、コンマを付け、重要な順に区切って、含める必要があります。例:

```
[rescue] mailbox = %y%¥antidote, c:¥antidote
```

スケジュール情報

Schedule Mode は、確認を表します。

表 61. スケジュール・モード

スケジュール・モード	
SCHED_NONE	0x000
SCHED_MINUTELY	0x001
SCHED_DAILY	0x002

表 61. スケジュール・モード (続き)

スケジュール・モード	
SCHED_WEEKLY	0x004
SCHED_MONTHLY	0x008
SCHED_STARTUP	0x010
SCHED_WAKEUP	0x020
SCHED_USB_ATTACH	0x040
SCHED_NETWORK_ATTACH	0x080

```
[Scheduler]
Task1=rescuerecovery
Task2=Rescue

[rescue]
ScheduleFrequency=0
ScheduleMode=0x02
TaskShow=1
Task=c:¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥adm¥mailman.exe
ScheduleHour=11
ScheduleMinute=28
ScheduleDayOfTheWeek=3
ScheduleWakeForBackup=0
```

署名キー

署名キーが使用される場合、それをクライアントに配布する必要があります。APKGMES コマンドによって作成されたファイル keyfile.pub にはキーが含まれます。認可された各公開署名キーは TVT.TXT ファイルで `pubkeyX = ...` として表示され (ここで *X* は整数によって置き換えられます)、最大 9 つの公開キーを格納できます。APUBKEY 機能を使用して、この値を `nosig =` と設定します。これが 1 に設定される場合、未署名パッケージ (/NOSIG パラメーターを使用して作成されたパラメーター) を実行させることができます。

注: 1 に設定されないか、公開キーが TVT.TXT ファイルにある場合、未署名パッケージは実行されません。

ネットワーク・ドライブ

以下の値は、AUNCPW の機能により `RscDrvY` セクション内に設定されます。各 `RscDrv` セクションには 1 つのネットワーク共有に関する情報が含まれます。最大 10 のネットワーク共有を Antidote Delivery Manager 用に定義できます。

- UNC = Antidote Delivery Manager が接続するべきドライブの UNC
- User = 暗号化されたユーザー名
- Pwd = 暗号化されたパスワード
- Ref = この接続に関連付けられる参照名

クライアントでのインストール

Rescue and Recovery 3.0 は、すべてのクライアントにインストールされている必要があります。上記で準備した設定は、インストール時に行うことができますが、後で実行しても構いません。

サーバー・インフラストラクチャー

管理者は、リポジトリー用のネットワーク共有を設定するか、FTP または HTTP サイトを提供する必要があります。修正およびパッチ用に追加のリポジトリーが必要になる場合があります。

単純なシステム・テスト - 通知の表示

スクリプトの準備およびパッケージ化

GO.RRS スクリプトを Antidote Delivery Manager をインストール済みのいずれかの PC に書き込みます。`MSGBOX /MSG "Hello World" /OK` という行を含むようにします。コマンドをコマンド・プロンプトから直接実行し、それが望みどおり機能していることを確認します。次に、GO.RRS を含むフォルダーで APKGMSG コマンドを実行してメッセージを作成します。メッセージ・ファイルを PC のリポジトリー・フォルダーのいずれか 1 つに配置し、正しく動作するか監視します。

デプロイメント

Antidote Delivery Manager をデプロイする前に、次のステップを実行します。

1. メールボックスの位置を決定します。
   - メールボックス は、ネットワーク共有、 HDD のローカル・システムまたは取り外し可能メディア、または FTP、HTTP サイトでディレクトリーとして定義されます。
   - 複数のメールボックスを所有していると、1 つのメールボックスにアクセスできない場合に便利です。メールボックスの位置を最大 10 まで定義できます。
   - ネットワーク・ベースのメールボックスは、クライアントで読み取り専用とし、書き込みアクセスを制限します。
2. TXT.TXT ファイルでメールボックスをセットアップします。
   - Rescue and Recovery をインストールしたドナー・システムで、*C:¥Program Files¥IBM¥ThinkVantage* ディレクトリーの TVT.TXT ファイルを編集します。
   - TVT.TXT ファイルに新規 レスキュー・セクションを作成します。
   - レスキュー・セクションに次の項目を追加します。

     ```
     mailbox=
     ```

     次にメールボックス・ディレクトリー情報を追加します。たとえばローカル・ドライブのメールボックスは次のようになります。

     ```
     [rescue]
     mailbox=C:¥ADM¥Mailbox,
     ¥¥Network¥Share
     ```

     FTP サイトのメールボックスは次のようになります。

     ```
     ftp://ftp.yourmailbox.com
     ```

     共有回線網ドライブのメールボックスは次のようになります。

     ```
     ¥¥Network¥Share
     ```

注:

a. HTTPS は、メールボックス機能ではサポートされていません。

b. HTTP Web サーバーは索引付けをオンにし、ファイルをリストする機能を配信するように構成する必要があります。

ドライブ名は、Windows Professional Edition およびご使用の通常オペレーティング・システム環境の間で変更される場合があります。最も変更される可能性が高いのは C: ドライブです。これを回避するには、環境変数 *CUSTOS* を使用します。これは常に標準的カスタマー・オペレーティング・システムを含むドライブをポイントします。前述の例は次のように変更されます。

```
mailbox=%CUSTOS%¥ADM¥Mailbox,ftp://ftp.yourmailbox.com, ¥¥Network¥Share
```

ストリングは、使用する装置またはプロトコルの標準に準拠する限り、どのような長さにもできます。たとえば、ローカル・ファイルを使用している場合、パスは 256 文字を超えることはできません。

- 複数メールボックス項目は、コンマまたはセミコロンで分離されます。
- Antidote Delivery Manager はパッケージの指定されたメールボックスの位置を順番に調べます。

3. FTP または HTTP 接続にユーザー名およびパスワードが必要な場合、次のフォーマットを使用します。

```
ftp//username:password@ftp.yourmailbox.com
```

4. ユーザー名とパスワードに応じて、ネットワークはメールボックスを共有します。

ユーザー名とパスワードの項目は、暗号化されて TVT.TXT ファイルに保管されます。ドナー・システムに項目を追加するには、次を実行します。

a. DOS ウィンドウを開きます。

b. ディレクトリーを C:¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥ADM に変更します。

c. 次のコマンドを実行します。

```
auncpw /add ¥¥Network¥Share /user username /pwd password /ref refID
```

このコマンドは TVT.TXT ファイルに次の項目を作成します。

```
[RscDrv0]
UNC=¥¥Network¥Share
 User=01E23397A54D949427D5AF69BF407D5C
Pwd=04E22197B34D95943ED5A169A0407C5C
Ref=refID
```

注:

a. この項目は、同じ共有へのアクセスを取得するため Antidote Delivery Manager によって使用されるあらゆるシステムで使用できます。

b. Antidote Delivery Manager は、最大 10 のネットワーク共有を使用できます。

c. 10 のネットワーク共有に加え、FTP または ローカルなど、その他のメールボックス項目を追加できます。

d. AUNCPW.EXE ファイルには、この他にパスワード管理に使用できる機能があります。コマンド・ラインで AUNCPW /? を入力するか、 193 ページの表 59 を参照してください。

5. Antidote Delivery Manager 公開/秘密鍵ペアを作成します。Antidote Delivery Manager の公開/秘密鍵ペア機能を使用することを推奨します。Antidote Delivery Manager は、公開/秘密鍵ペアを使用してパッケージの認証性を検査します。秘密鍵は確実に保護し、分散しないようにします。一致する公開鍵は、 Antidote Delivery Manager で管理される各クライアントになくてはなりません。インストールされた Rescue and Recovery で非ドナー・システムに公開/秘密鍵ペアを作成するには、次を実行します。

   a. DOS ウィンドウを開きます。

   b. C:¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥ADM に CD コマンドを発行します。

   c. 次のコマンドを実行します。

   ```
   apkgmes.exe /newkey mykey
   ```

   このコマンドは、mykey.pub および mykey.prv の 2 つのファイルを作成します。順に、公開鍵、秘密鍵です。

   d. ドナー・システムの C:¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥ADM ディレクトリーに公開鍵をコピーします。

   e. notepad.exe などのテキスト編集プログラムを使用してファイルを開きます。

   f. クリップボードにファイルの内容をコピーします。

   g. コマンド・ラインに以下を入力します。

   ```
   apubkey.exe /add x
   ```

   ここで *x* はクリップボードの内容です。

   h. これにより、「レスキュー」セクションの TVT.TXT に項目が作成されます: `pubkey0=906253...`。

   - 最大 10 の公開鍵を TVT.TXT に保管できます。
   - APUBKEY.EXE ファイルには、公開鍵管理に使用できる別の機能があります。コマンド・ラインで `APUBKEY /?` と入力するか、 193 ページの表 59 を参照します。

6. Schedule Antidote Delivery Manager チェックを作成します (複数のスケジュールを許可)。Antidote Delivery Manager はシステムで定期的に実行する必要があります。20 分ごとに実行するスケジュールをセットアップするには、ドナー・システムの TVT.TXT ファイルに以下を追加します。

   ```
   [Scheduler]
   Task1=rescuerecovery
   Task2=egatherer
   Task3=rescue

   [rescue]
   ScheduleFrequency=0
   ScheduleMode=0x01
   NumMinutes=20
   TaskShow=1
   Task=C:¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥ADM¥antidote
   ¥mailman.exe
   ```

ここで *ScheduleMode* は Antidote Delivery Manager パッケージの配信をトリガーするイベントです。パラメーターは次のとおりです。

表 62. Antidote Delivery Manager パラメーター

パラメーター	値
SCHED_NONE	0x000
SCHED_MINUTELY	0x001
SCHED_DAILY	0x002
SCHED_WEEKLY	0x004
SCHED_MONTHLY	0x008
SCHED_STARTUP	0x010
SCHED_WAKEUP	0x020
SCHED_USB_ATTACH	0x040
SCHED_NETWORK_ATTACH	0x080

注:

a. スケジューラーは Rescue and Recovery ワークスペースで稼働しません。

b. 詳しくは、 168 ページの『バックアップおよび関連タスクのスケジューリング』を参照してください。

7. Antidote Delivery Manager パッケージを作成します。

   ここまでのステップを完了したら、ご使用の最初のパッケージをビルドし、配布します。管理者システム (非ドナー) で、以下を実行します。

   a. *C:¥ADM¥Build* などのディレクトリーを作成します。

   b. そのディレクトリーで、GO.RRS という名前のファイルを作成し、以下を追加します。

   ```
   msgbox.exe /msg "Hello World!" /head "test" /ok /cancel
   ```

   c. ファイルを保存してクローズします。

   d. C:¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥ADM に CD コマンドを発行します。

   e. 次のコマンドを実行します。

   ```
   apkgmes.exe /key mykey.prv C:¥adm¥build HELLOPKG
   ```

   f. これにより HELLOPKGYY*MMDDHHMM*.ZAP という名前のパッケージが作成されます。ここで *MMDDHHMM* は現在日時に置き換えられます。

8. HELLOPKGYY*MMDDHHMM*.ZAP をステップ 2 で指定したメールボックスの位置にコピーします。

9. Antidote Delivery Manager を起動します。

   a. ドナー・システムのタイマーが期限切れになると、パッケージが稼働し、「Hello World」メッセージ・ボックスが表示されます。

   b. 待ちたくない場合は、ドナー・システムで C:¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥ADM¥mailman.exe を入力することができます

例

以下は Antidote Delivery Manager の使用例です。

例 1

これは、レジストリーにあるウィルスまたは不正項目のため、常に青色の画面となっている PC を修正するパッケージの例です。

1. クライアント PC が青色の画面を表示している原因は、レジストリーの Run キーを通じて感染したウィルスによるものと仮定します。これを修正するには、*reg* を実行する、go.rrs という名のファイルを作成する必要があります。Microsoft コマンドのリストについては、 197 ページの『サポートされる Microsoft コマンド』を参照してください。可能であれば、reg からレジストリー値を削除し、システムから実行可能ファイルを削除します。内容は次のようになります。

   ```
   reg delete HKLM¥Software¥Microsoft¥Windows¥Current Version¥Run /v runvirusvalue
   /f del %custos%¥windows¥system32¥virus.exe
   ```
2. ご使用の *c:¥adm¥build* ディレクトリーに go.rrs ファイルを置き、以下を実行します。

   ```
   apkgmes.exe /key mykey.prv C:¥adm¥build REMOVEVIRUS
   ```
3. ご使用のメールボックスに REMOVEVIRUS*YYDDHHMM*.ZAP をコピーします。
4. それぞれのクライアントをブートし、「ThinkVantage」ボタン、「Access IBM」ボタン、F11 または Enter キーを押して Rescue and Recovery ワークスペースに移動します。開始時に mailman.exe ファイルが実行され、次に REMOVEVIRUS パッケージが実行されます。

例 2

この例では、Quick Fix Engineering 更新を強制するか、またはクライアント にパッチを当てます。

1. *C:¥adm¥patchbuild* のような、スクリプト・ファイルとパッチ・ファイルを保留するディレクトリーを作成します。
2. c:¥adm¥patchbuild ディレクトリー に qfe または パッチ実行可能ファイルを置きます。
3. go.rrs という名のファイルを作成し、そこに次の行を置きます。ただし、Microsoft Quick Fix Engineering またはパッチを実行しインストールする行をカスタマイズします。 このパッチは通常の Windows オペレーティング・システムにしかインストールできないので、このスクリプトはインストールが Windows Professional Edition で実行されないようにします。

   ```
   set custos
   if errorlevel 1 set custos=%systemDrive%
   %custos%¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥ADM¥retryonerror
   /on 10
   %custos%¥Program Files¥IBM ThinkVantage¥Rescue and Recovery¥ADM¥InRR.exe
   if errorlevel 2 goto ERROR
   if errorlevel 1 goto InOS
   if errorlevel 0 goto InPE

   :ERROR
   exit 1

   :InOS
   REM DISABLE NETWORKING
   ```

```
Netwk.exe /d
patchinstall.exe
REM ENABLE NETWORKING
Netwk.exe /e
msgbox.exe /msg "Patch Installed" /head "Done" /ok
exit 0

:InPE
exit 1
```

4. go.rrs を c:¥adm¥patchbuild ディレクトリーに置き、実行します。

   ```
   apkgmes.exe /key mykey.prv C:¥adm¥patchbuild PATCHBUILD
   ```

5. ご使用のメールボックスに PATCHBUILD*YYDDHHMM*.ZAP をコピーします。
6. パッチは、クライアント PC の mailman.exe ファイルの次の実行時、またはクライアント PC の再起動時にインストールされます。

パッケージが完了しているかどうかを確認する方法

- **失敗ログ**

  このファイルは通常 *c:¥ibmtools¥utils¥rescue¥* ディレクトリーに保管されます。ゼロ以外の値を持つ .zap ファイルが終了する場合、このファイルにログされます。

- **Rescue.log**

  このファイルは通常 *c:¥ibmshare* ディレクトリーに保管されます。このファイルは、パッケージが失敗した理由、またはパッケージを作動させる方法を判別するのに役立つ詳細情報を提供します。このファイルは、.zap ファイルでの現象を行ごとにロギングしています。

- **成功ログ**

  このファイルは通常 *c:¥ibmtools¥utils¥rescue¥* ディレクトリーに保管されます。.zap ファイルがゼロの値で終了する場合、ここにログされます。

例 3

この例は Rescue and Recovery ワークスペースの FTP または HTTP サイトを使用します。

1. 以下のパッケージ用に、外部 Web サイトを定義する。

   ```
   ftp.yourmailbox.com
   ```

2. 公開および秘密鍵を作成する。ステップ 5 を参照してください。
3. TVT.TXT にメールボックスを追加します。

   ```
   mailbox=ftp://username:password@ftp.yourmailbox.com
   ```

4. PreDesktopArea に入るため、ユーザーが Access IBM/F11 または Enter キーを押すと、ブート時に Antidote Delivery Manager パッケージが Rescue and Recovery ワークスペースで実行します。

例 4

この例は、特定のクライアントをターゲットにした xmltool.exe ファイルを使用します。

1. アクティブ・ディレクトリー、Systems Management Server またはその他の管理ツールを通して、ご使用のクライアント PC と比較したい情報を含む XML ファイルを配布します。

```
<file>
<activedirgroup>Marketing</activedirgroup>
</file>
```

2. go.rrs ファイルの最初の行に、xml ツールを使用する行を置きます。この行は、Marketing グループ内の PC をターゲットにするのみの例です。

```
xmltool.exe c:¥mycompany¥target.xml //file/activedirgroup /c EQU Marketing
if errorlevel 0 goto RUNIT
exit errorlevel

:RUNIT
#place code to execute patch or whatever action
```

大規模なワームの攻撃

次の例では、主要なウィルスに対抗するための考えられるアプローチの 1 つを明示します。基本的なアプローチは、ネットワークをオフにしてから、再起動して Rescue and Recovery に入り、レジストリーを修復し、置換ファイルを所定の場所にコピーしてから、起動して Windows XP に戻り、ネットワークを復元します。説明のために、下記のアプリケーションは改訂された構文に更新する必要があります。

Go.RRS

```
set tagfile=1.tag
set pingtarg=192.168.1.1
retryonerror /on 10
set custos
if errorlevel 1 set custos=%systemDrive%

cd %custos%¥ibmtools¥utils¥rescue¥dne¥work

inRR.exe
if errorlevel 2 goto ERROR
if errorlevel 1 goto InOS
if errorlevel 0 goto inRR

:InOS
cd
if exist %tagfile% goto DONE

msgbox /msg "Antidote has detected a new message ¥n  ¥n ..... ¥n  ¥n Don't worry; be Happy!
Antidote will fix your system for you" /ok /timer 30
call nettest.cmd %pingtarg%
set el=%errorlevel%
if %el% == 0 msgbox /msg "Network is working" /timer 5 /head "Correct"
if not %el% == 0 msgbox /msg "Network is disabled" /timer 5 /head Failure
NetWk.exe /d
msgbox.exe /msg "Antidote Recovery Process is running. ¥n  ¥n Networking has been disabled." /head
"Networking" /timer 15
call nettest.cmd %pingtarg%
set el=%errorlevel%
if %el% == 0 msgbox /msg "Network is working" /timer 5 /head "Failure"
if not %el% == 0 msgbox /msg "Network is disabled" /timer 5 /head "Correct"
msgbox.exe /msg "System will reboot in 20 seconds ¥n  ¥n Press OK to reboot now, or Cancel to
reboot later."
/head "Select Repair Urgency" /timer 20 /ok /cancel
if errorlevel 2 goto PENOW
if errorlevel 1 goto PELATER
if errorlevel 0 goto PENOW

:PENOW
reboot /rr
goto NOT_DONE
```

```
:PELATER
%custos%¥ibmtools¥utils¥bmgr32.exe ¥bw
msgbox.exe /msg "System will apply fix next time you reboot" /head "Reboot" /ok
goto NOT_DONE

:inRR
REM DISABLE NETWORKING
msgbox.exe /msg "Networking will be disabled in 5 seconds. ¥n  ¥n  Network disable pending"
/head "Network shutdown" /timer 5
NetWk.exe /d

REM USE EGATHERER VALUES FOR CONDITIONAL BRANCH

msgbox /msg "Checking Registry" /timer 5
xmltool %ibmshare%¥ibmegath.xml //EG_GATHERED_DATA/EG_INSTALLED_MICROSOFT_SOFTWARE/
EG_SOFTWARE_PACKAGE[@ID='DirectX']/EG_VERSION GEQ ¥"4.09.00.0901¥"
if errorlevel 1 goto FILECOPY

msgbox.exe /msg "Applying Registry fix. ¥n  ¥n Press OK to continue..." /head "Registry Fixeroo" /ok
reg.exe load HKLM¥tempSW %custos%¥windows¥system32¥config¥SOFTWARE
reg.exe add "HKLM¥tempSW¥IBM¥eGatherer¥Local Viewer¥scans¥banka" /v benke /d binki /f
reg.exe add "HKLM¥tempSW¥IBM¥eGatherer¥Local Viewer¥scans¥banka" /v bonko /d bunku /f
reg.exe delete "HKLM¥tempSW¥IBM¥eGatherer¥Local Viewer¥scans¥banka" /v bonko /f
reg.exe unload HKLM¥tempSW

:FILECOPY
msgbox /msg "Registry Now OK ¥n  ¥n Applying Fix" /timer 5
copy payload.txt %custos%¥

REM RE-ENABLE NETWORK
msgbox.exe /msg "Networking will be enabled in 5 seconds. ¥n  ¥n Network enable pending" /head
"Network shutup" /timer 5
NetWk.exe /e

REM TAG IT
echo 1 > %tagfile%

REM REBOOT
msgbox.exe /msg "System will reboot in 5 seconds..." /head "Reboot..." /timer 5
reboot.exe
goto NOT_DONE

:ERROR
:NOT_DONE
exit 1

:DONE
NetWk.exe /e
msgbox.exe /msg "Fix Applied ¥n  ¥n You may now continue normal operation."
/head "Done" /ok
exit 0
```

NETTEST.CMD

```
PING -n 1 %1 > nul 2>&
```

PAYLOAD.TXT

```
a test file
of a payload to deliver.
```

付録 G. 特記事項

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、レノボ・ジャパンの営業担当員にお尋ねください。本書で Lenovo 製品、プログラム、またはサービスに言及していても、その Lenovo 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、Lenovo の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、Lenovo 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

Lenovo は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

Intellectual Property Licensing
Lenovo Group Ltd.
3039 Cornwallis Road
Research Triangle Park, NC 27709
U.S.A.
Attention: Dennis McBride

Lenovo およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 Lenovo は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書で説明される製品は、誤動作により人的な傷害または死亡を招く可能性のある移植またはその他の生命維持アプリケーションで使用されることを意図していません。本書に記載される情報が、Lenovo 製品仕様または保証に影響を与える、またはこれらを変更することはありません。本書におけるいかなる記述も、Lenovo あるいは第三者の知的所有権に基づく明示または黙示の使用許諾と補償を意味するものではありません。本書に記載されるすべての情報は、特定の環境において得られたものであり、例として提示されます。他の操作環境で得られた結果は、異なる可能性があります。

Lenovo は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本書において Lenovo 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この Lenovo 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

商標

以下は、Lenovo Corporation の商標です。

Lenovo
Rescue and Recovery
ThinkPad
ThinkCentre
ThinkVantage
Rapid Restore

Intel® は Intel Corporation またはその子会社の米国およびその他の国における商標または登録商標です。

IBM、Lotus®、および Lotus Notes® は、 IBM Corporation の商標です。

Microsoft、Windows および Windows NT® は Microsoft Corporation の米国およびその他の国における商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

用語集

管理者 (ThinkCentre)/ スーパーバイザー (ThinkPad) BIOS パスワード. 管理者パスワードまたはスーパーバイザー・パスワードは、BIOS 設定を変更する能力を制御するために使用される。これには、エンベデッド・セキュリティー・チップを使用可能/使用不可にして、TPM 内に保管されたストレージ・ルート鍵をクリアする機能が含まれる。

Advanced Encryption Standard (AES). *Advanced Encryption Standard* は対称鍵暗号化技法。アメリカ政府は、それまで使用していた DES 暗号化に置き換えて、このアルゴリズムをその暗号化技法として 2000 年 10 月に採用。 AES は、凶暴なアタックに対して 56 ビット DES キーよりも高度のセキュリティーを提供する。また AES では、必要に応じて 128、192 および 256 ビット・キーの使用が可能。

暗号化システム (Cryptography system). 暗号化システムは、データの暗号化と復号の両方を行う単一の鍵を使用する対称鍵暗号化と、2 つの鍵 (全員に知られている公開鍵と鍵ペアの所有者のみがアクセス権を持つ秘密鍵) を使用する公開鍵暗号化に、大きく分類される。

エンベデッド・セキュリティー・チップ. エンベデッド・セキュリティー・チップは、TPM の別名。

公開鍵/非対称鍵暗号化 (Public-key/Asymmetric-key encryption). 公開鍵アルゴリズムは通常、2 つの関連した鍵のペアを使用する。1 つは秘密に保持されなければならない秘密鍵で、もう一方は公開される鍵で広く配布される。鍵が 1 つあった場合、ペアのもう一方が推測できるようであってはならない。「公開鍵暗号化」という用語は、鍵の一部を公開情報にするというアイデアから得られる。すべてのパーティーが同じ情報を保持しないことから、非対称鍵暗号化という用語も使用される。ある意味では、1 つの鍵がロック (暗号) を「ロック」し、別の鍵はそれをアンロック (復号) することを要求される。

ストレージ・ルート鍵 (SRK). ストレージ・ルート鍵 (SRK) は 2,048 ビット (あるいはそれ以上) の公開鍵ペア。これは最初は空で、TPM 所有者が割り当てられたときに作成される。この鍵ペアは、エンベデッド・セキュリティー・チップをそのままでは放置しない。 TPM の外部にあるストレージの秘密鍵を暗号化 (ラップ) し、TPM にロード・バックされたときにそれらを復号する。 SRK は、BIOS にアクセスのある人なら誰でもクリアすることができる。

対称鍵暗号化 (Symmetric-key encryption). 対称鍵暗号化暗号はデータの暗号化と復号に同じ鍵を使用する。対称鍵暗号は簡単で高速だが、主な欠点は、2 つのパーティーが何らかのセキュアな方法で鍵を交換しなければならないことにある。公開鍵暗号化は、公開鍵は非セキュアな方法で配布可能であり、秘密鍵は転送されることがないので、この問題を回避している。 Advanced Encryption Standard は対称鍵の一例。

TPM (Trusted Platform Module). TPM は特別な目的を持ってシステム内にビルドされた集積回路で、強力なユーザー認証と PC 検査を可能にする。 TPM の主な目的は、機密情報への不適切なアクセスを防止することにある。 TPM はハードウェア・ベースの信頼の基幹機能で、システム上のさまざまな暗号サービスを提供するように活用することができる。 TPM の別名はエンベデッド・セキュリティー・チップ。

ThinkVantage

Printed in Japan